NAVAL POSTGRADUATE SCHOOL
Monterey, California

THESIS

ELECTRONIC COMMERCE: AN ANALYSIS OF FINANCIAL TRANSACTION METHODS AND ASSOCIATED SECURITY

by
David Kenneth Flick Sr.
and
Charles Royce Gillum Jr.
September 1996

Principal Advisor: William J. Haga

Approved for public release; distribution is unlimited.

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.

1. AGENCY USE ONLY *(Leave blank)*

2. REPORT DATE September 1996

3. REPORT TYPE AND DATES COVERED Master's Thesis

4. TITLE AND SUBTITLE Electronic Commerce: An Analysis of Financial Transaction Methods and Associated Security

5. FUNDING NUMBERS

6. AUTHOR(S) David Kenneth Flick Sr. and Charles Royce Gillum Jr.

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited.

12b. DISTRIBUTION CODE

13. ABSTRACT *(maximum 200 words)*

This study examines an obstacle to commerce on the Internet and the World Wide Web posed by a popular belief that the Internet and Web lack the technology needed for secure financial transactions. The reality behind such a belief has a direct effect upon commercial and financial transactions by DOD in view of an Executive Order that mandates Internet usage for electronic transactions. This study details and evaluates the methods available for secure financial transactions on the Internet. Each transaction method analysis provides security protocol functionalities, advantages and disadvantages and company profiles. The study also details the impediments to using the World Wide Web as a commercial medium. It concludes that the popular belief is unfounded. Implications are drawn for DOD practices and policy. DOD and the entire U.S. federal government has a stake in the Internet's capability to process secure financial transactions.

14. SUBJECT TERMS
Electronic Commerce Security

15. NUMBER OF PAGES 188

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT
Unclassified

18. SECURITY CLASSIFICATION OF THIS PAGE
Unclassified

19. SECURITY CLASSIFICATION OF ABSTRACT
Unclassified

20. LIMITATION OF ABSTRACT
UL

ELECTRONIC COMMERCE: AN ANALYSIS OF FINANCIAL TRANSACTION METHODS AND ASSOCIATED SECURITY

David Kenneth Flick Sr.
Lieutenant, United States Navy
B.S., United States Naval Academy, 1988
and
Charles Royce Gillum Jr.
Lieutenant, United States Navy
B.S., United States Naval Academy, 1990

Submitted in partial fulfillment
of the requirements for the degree of

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
September 1996

Authors: D Kenneth Flick
David Kenneth Flick Sr.

Charles R Gillum
Charles Royce Gillum Jr.

Approved by: William J Haga
William J Haga, Principal Advisor

Barry Frew
Barry A. Frew, Associate Advisor

for
Reuben T. Harris, Chairman Department of Systems Management

ABSTRACT

This study examines an obstacle to commerce on the Internet and the World Wide Web posed by a popular belief that the Internet and Web lack the technology needed for secure financial transactions. The reality behind such a belief has a direct effect upon commercial and financial transactions by DOD in view of an Executive Order that mandates Internet usage for electronic transactions. This study details and evaluates the methods available for secure financial transactions on the Internet. Each transaction method analysis provides security protocol functionalities, advantages and disadvantages and company profiles. The study also details the impediments to using the World Wide Web as a commercial medium. It concludes that the popular belief is unfounded. Implications are drawn for DOD practices and policy. DOD and the entire U.S. federal government has a stake in the Internet's capability to process secure financial transactions.

TABLE OF CONTENTS

I. INTRODUCTION

The number of Internet hosts has significantly increased since its development by the Department of Defense. The number of Internet hosts connected in August 1981 was 213 (Internet Society, 1996). This number has grown to 12.88 million hosts in July 1996 and is projected to reach 33.96 million by January 1998 (Internet Society, 1996). The number of Internet users in 1996 is estimated to be 9.8 million (O'Reilly, 1996). This number is expected to increase five times to 52 million by the year 2000 (Forrester, 1995).

The explosion in the number of hosts being connected to the Internet is accelerating the trend towards business use of open networks for conducting electronic commerce (Roche, 1995). More than 80,000 companies use the Internet for distribution of critical company information (Roche, 1995). Retail sales on the Internet reached $350 million in 1995. This figure is projected to reach $6.9 billion by the year 2000 (Eicher and Modahl, 1995). Still, these numbers are insignificant when compared to other markets. For instance, the print catalog industry reached $57 billion in 1995 (Kline, 1995) and global credit card sales totaled $3 trillion in 1995 (Lister, 1996).

Several barriers are preventing electronic commerce from achieving its full potential as a commercial medium. Security is the primary obstacle to electronic commerce. Surveys have found that users cite security concerns as the number one reason for not buying merchandise on the Internet. They feel that their credit card numbers can be easily stolen while being transmitted over the Internet (Faulkner & Gray Inc., 1995; Gupta, 1996; Jaffee, 1996). However, the reality is that financial transactions on the

Internet are safe. They are as secure or more secure than conventional credit card transaction methods, especially when encryption is used (Busch, 1996; Dahl, 1995; Forrester, 1996; Grossman, 1996; Kline, 1995; Lynch, 1996; Netscape, 1996; Power, 1996; Roche, 1995; Wilson, 1996). Other barriers which are limiting the growth of electronic commerce include access and speed (Wilson, 1996), the absence of online dynamic content directories (Hoffman et al., 1996), time required to download Web site graphics (Gupta, 1996), lack of sites that offer transactions online (Gens, 1996), and startup costs to businesses (Connect, 1996).

The Department of Defense, of course, developed what is now called the Internet and is a major user of its communication capacity. It follows, then, that the DOD and the entire U.S. federal government has a stake in the Internet's capability to process secure financial transactions. This is particularly true where DOD or other agencies are receiving payments, making payments or communicating sensitive documents such as bids. This need for communication security will grow as more agencies and commands solicit bids from a geographically broad market of vendors through Web sites on the World Wide Web. This thesis performs a comprehensive analysis of the available financial transaction methods and associated security protocols.

II. SIZE AND GROWTH OF THE INTERNET AND WORLD WIDE WEB

A. INTERNET HOSTS

When trying to measure the size and growth of the Internet, people usually think in terms of number of users. However, the first attempts at measuring the size of the Internet were aimed at counting the number of computers connected to the Internet. This number is both obtainable and measurable (Wiggins, 1995). A computer connected to the Internet is referred to as a "host" or "node" on the network (Wiggins, 1995). Hosts were relatively easy to count in the early stages of the Internet (i.e. early 1980's), they were listed in a special Host Table File which was distributed to Internet sites (Wiggins, 1995). This system became impractical when thousands of new hosts started to join the Internet. The growth in the number of hosts called for a distributed name database, allowing any user anywhere on the Internet to locate any other computer. This was the birth of the Domain Name System (DNS). The DNS is the part of the Internet that allows users to refer to hosts by names like www.nps.navy.mil instead of referring to IP addresses (Wiggins, 1995).

Lotter (Network Wizards, 1996) has conducted periodic surveys of the Domain Name System since 1981. Figure 1 illustrates the growth in IP addresses registered from 1989-1995. A complete list of host surveys from 1981 projected through the year 2000 is provided in appendix B (Internet Society, 1995). Appendix B also shows the most recent survey conducted in July 1996 that details number of hosts, domains, and networks (Network Wizards, 1996).

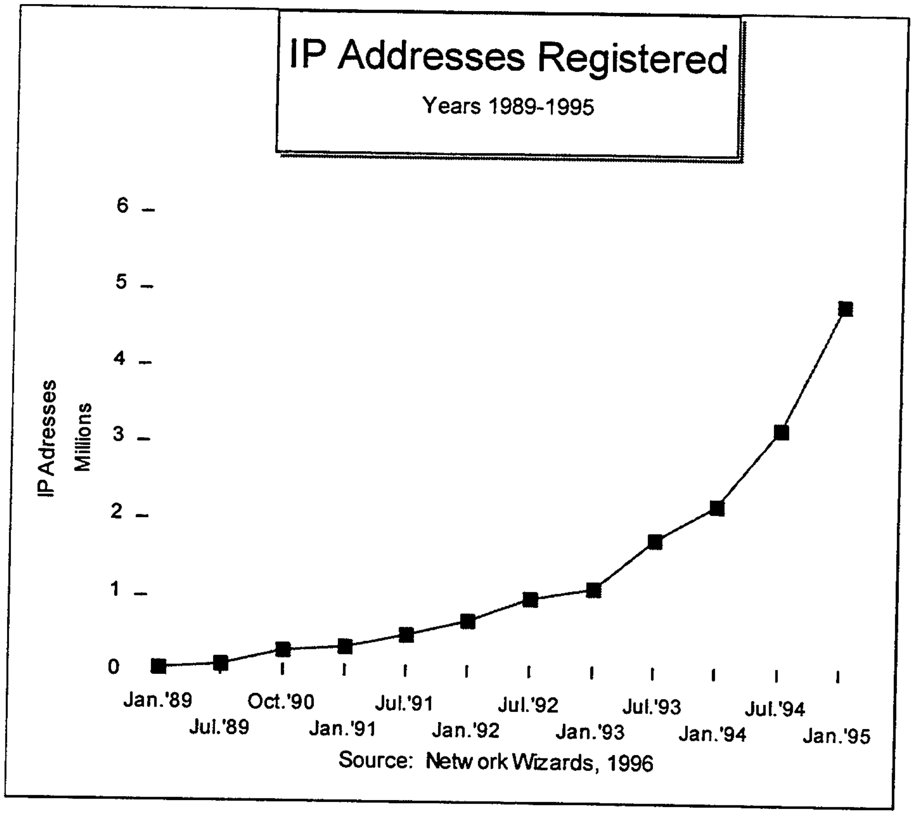


Figure 1: IP Addresses Registered   Source: Mark Lottor Surveys

Although these survey results give an accurate picture of the growth of the Internet, they still only represent a rough census at any given time. Some organizations have a habit of registering hosts before they actually connect to the Internet. Another common occurrence is a large percentage of registered hosts being down at any given time (Wiggins, 1995). A recent problem with Lottor's survey is the growing number of organizations who run their computers behind firewalls. This security practice obscures their presence on the Internet from the DNS and surveys (Wiggins, 1995).

The host surveys also give an idea of the domain growth on the Internet. Figure 2 shows the relative growth of different domains on the Internet in June 1994 (Internet Society, 1995).

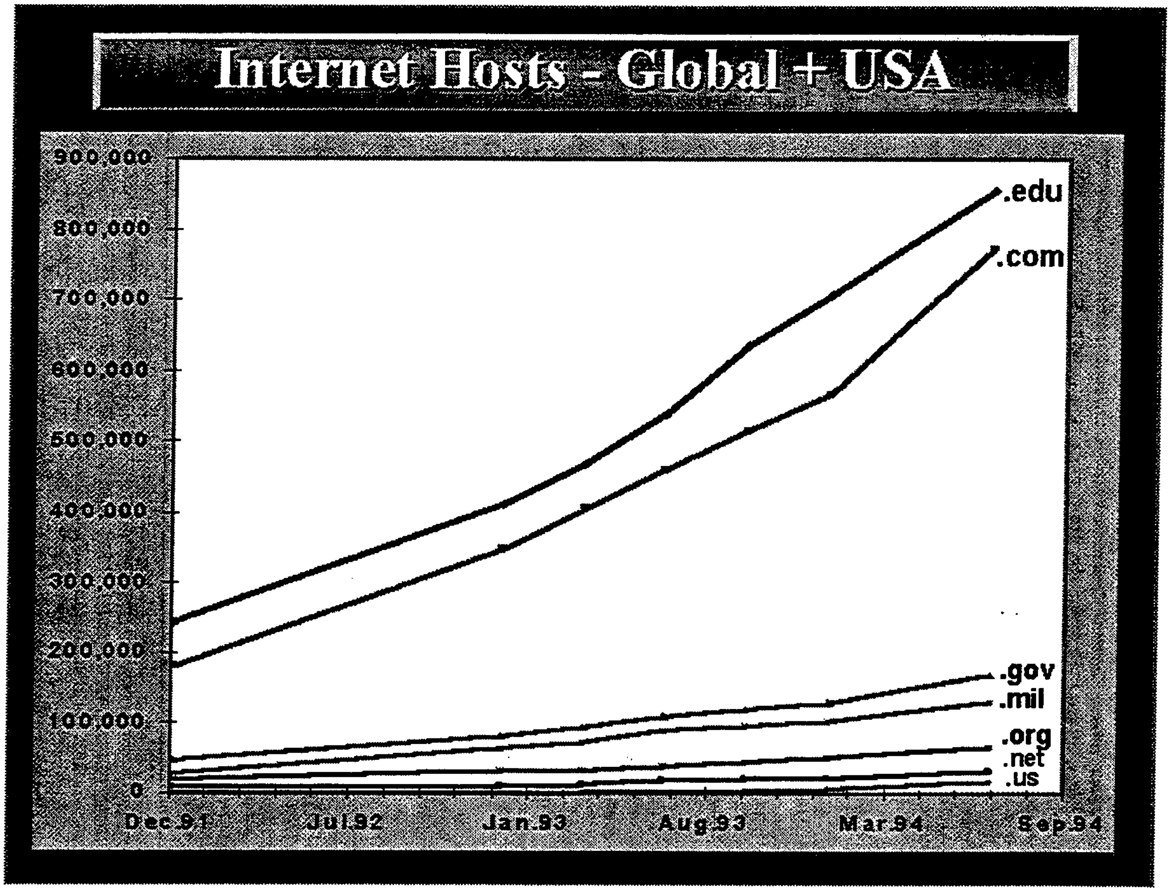


Figure 2: June 1994 Domain Breakdown Source: Internet Society, 1996

It is interesting to note that the domains such as .com (commercial) and .edu (educational) comprise a majority of the host domains. It is enlightening to see the educational domain leading all other domains. However, as Figure 3 shows, the commercial domain surpassed the educational domain in the number of hosts in January 1995 (Wiggins, 1995). The survey of July 1995 found that there were 6.64 million host computers on the Internet (Network Wizards, 1995). This number has been approximately doubling annually since 1981 (Hoffman et al., 1995).

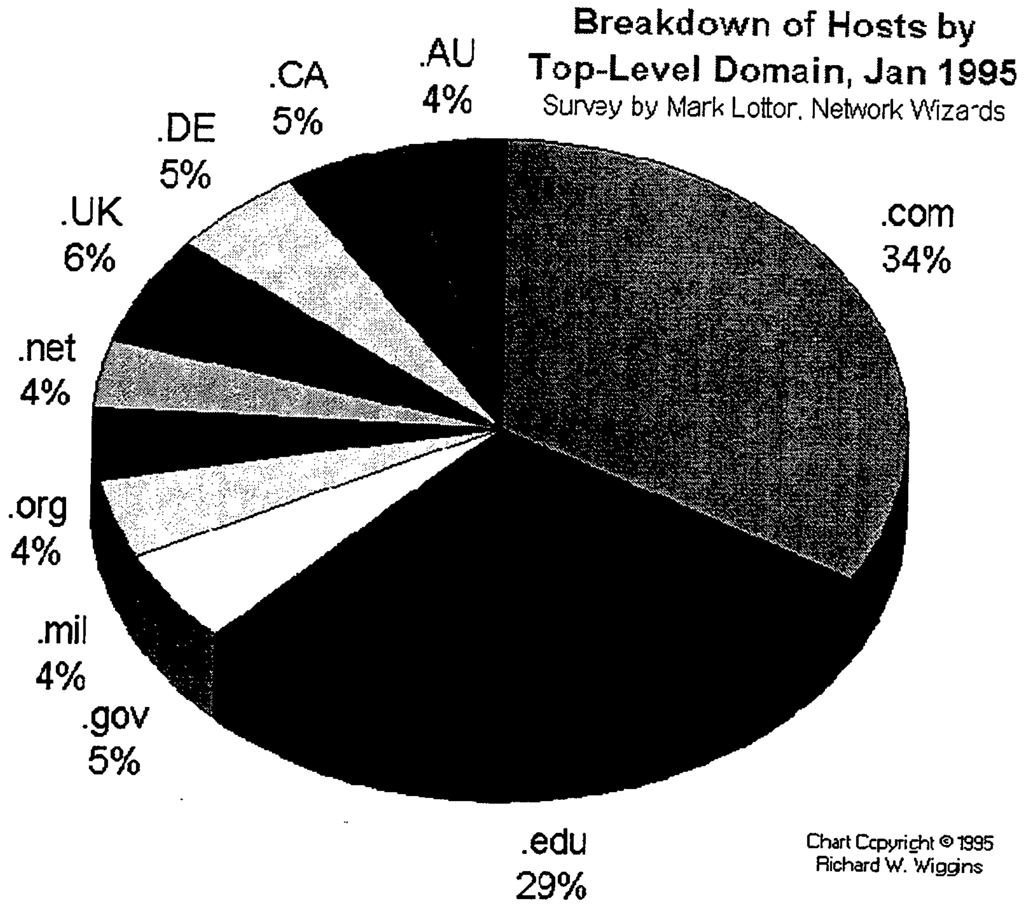


Figure 3: January 1995 Domain Breakdown

The domain breakdown of the July 1995 survey are shown in the table below:

Domain Type	Number of Hosts
.com	1.74 million
.edu	1.41 million
.net	0.30 million
.gov	0.27 million
.mil	0.22 million
.org	0.20 million

Demonstrating that the Internet is truly global, the same source indicated that 2.37 million of these are international hosts representing 150 countries (Hoffman et al., 1995).

The most recent domain survey was conducted July 1996 and is shown in Appendix B. It shows 12.88 million hosts on the Internet (Network Wizards, 1996). This number is nearly double the July 1995 figure of 6.64 million hosts (Network Wizards, 1996). The number of domains on the Internet has also grown. This survey shows 488,000 domains on the Internet in July 1996 which is over four times the 120,000 domains measured in July 1995 (Network Wizards, 1996).

The growth in the number of Internet-connected networks has also significantly increased. Appendix B shows that in August 1988 there were 208 networks in the United States and 9 networks connected to the Internet outside the United States (Internet Society, 1995). Figure 4 shows network growth between 1990 and 1994:

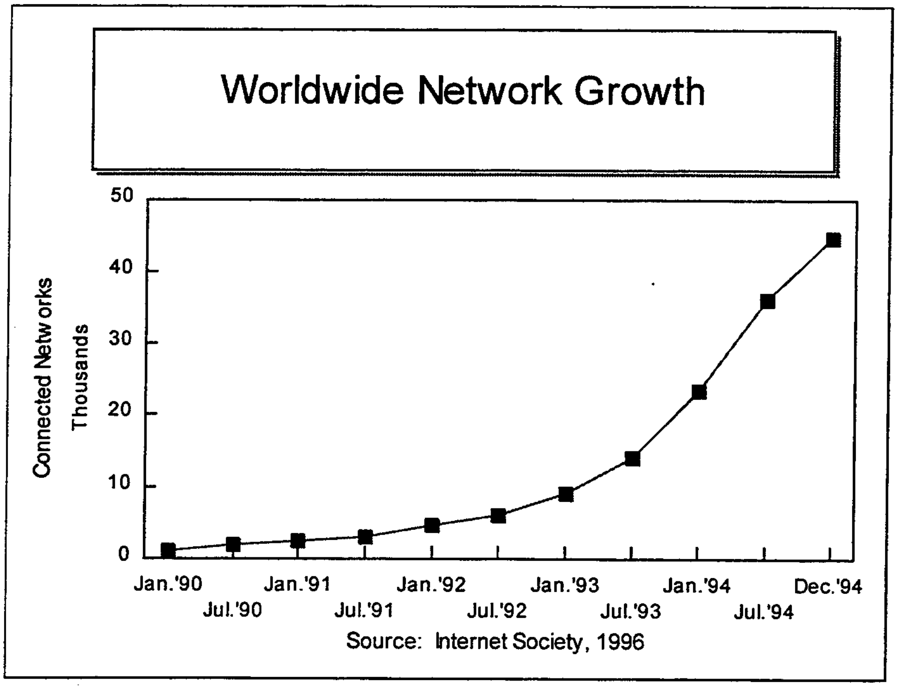
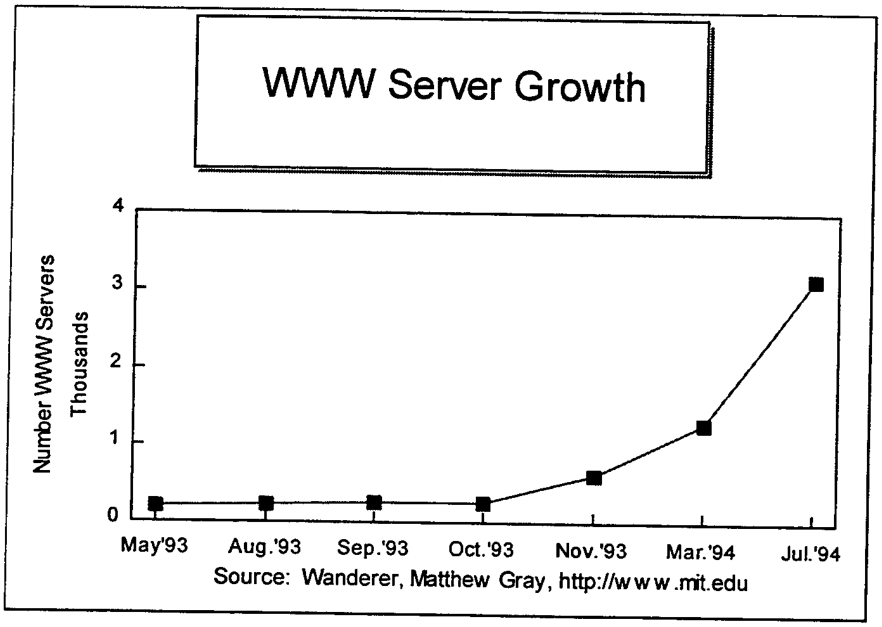


Figure 4: Network Growth

The most recent figures indicate that in January 1995 there were 26,681 networks in the U.S. and 19,637 networks outside the U.S. for a total of 46,318 networks connected to the

Internet worldwide (Internet Society, 1995). Internet Society projects that this number will increase to 103,553 networks in the U.S. and 91,269 networks outside the U.S. for a total of 194,822 networks worldwide by October 1996 (Appendix B).

The growth of World Wide Web sites is even more impressive than that of the Internet; the Web grew over 17 times in 1994 alone and doubles in size roughly every two to three months (Hoffman et al., 1995). Figure 5 represents Web server growth in 1993 and 1994.



Source: Wanderer, Matthew Gray, http://w w w .mit.edu

Figure 5: WWW Server Growth

Another indication of the relative growth of the Web is to compare it with gopher which is another Internet browser application. Figure 6 below represents this comparison. The search engine Lycos indexed 8.54 million unique URLs as of October 7, 1995 (Hoffman et al., 1995). This figure demonstrates the increasing content of Web servers. Statistics show that Web traffic now dominates Internet activity. The Web

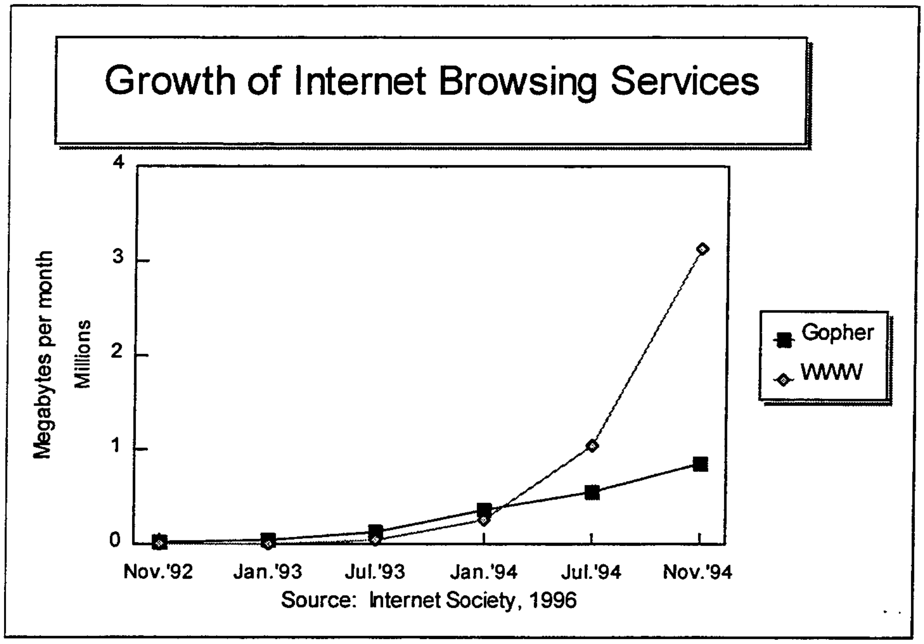


Figure 6: Web Tool Comparison

accounted for 21.4% of total packet traffic and 26.25% of total byte traffic in April 1995, ranking first among all networks on the Internet (Merit Network Inc., 1995).

B. INTERNET USERS

Determining the number of users on the Internet is more difficult than counting the number of computers connected to the Internet. Early estimates of the number of Internet users stemmed from host number calculations. The rule of thumb was 10 users for every host (Wiggins, 1995). This may have been a good estimate in the mid 1980's when mainframes and minicomputers dominated, but now that personal computers and workstations are connected directly to the Internet, it is common for one IP address to correspond with one user (Wiggins, 1995).

Campbell pointed out that in order to estimate total numbers of Internet users, the term Internet user must be defined (Wiggins, 1995). There are many parts of the Internet that can be used separately, ranging from e-mail to the Web to applications such as FTP and gopher (Wiggins, 1995). Several studies have estimated the number of Internet users and all have come up with different figures. It would appear that these results would be difficult to reconcile. Closer examination suggests that, apart from methodological flaws or survey bias, the differences are reconciled, at least in part, by understanding what is meant by Internet use (Hoffman et al., 1996).

The first extensive user demographic survey was conducted by Texas Internet Consulting (Matrix News, 1995). It was the first to understand the importance of defining an Internet user. It proposed three categories of Internet users. The first category was the "Core Internet." Core users were estimated at 7.8 million users of 2.5 million computers that can provide interactive services such as TELNET, FTP, or WWW and are capable of serving information on the Internet (Matrix News, 1995). The second category was the "Consumer Internet" user. Consumer Internet users comprise an estimated 13.5 million users of 3.5 million computers that can use the interactive services such as FTP or WWW supplied by the Core Internet. The on-line services AOL, Delphi, and Bix were included in this estimate (Matrix News, 1995). This user group can browse but not serve information. The final user group was defined as the "Matrix." Matrix users can exchange electronic mail with other users. The Matrix group is estimated to have 27.5 million users (Matrix News, 1995).

The Texas Internet Consulting survey later projected their results through September 1995. The projection yielded estimates of 22.6 million Consumer Internet users and 35 million Matrix users (Matrix News, 1995). Mass market utilities like CompuServe, Prodigy, American Online, and Delphi offer some forms of Internet access. This estimate is as high as 25%, yielding an overall Consumer Internet user population of 29 million (Wiggins, 1995).

The Texas Internet Consulting survey sent questionnaires by electronic mail to most of the domains representing organizations on the Internet (Matrix News, 1995). This methodology included using the July 1994 Lottor DNS survey to obtain a list of 18,473 domains (Matrix News, 1995). This survey took place exclusively through electronic mail. This presents a bias toward users of electronic mail, often causing inflated estimates. Several earlier surveys, Hermes for example, used online questionnaires which caused the data to be non-representative and used only for ballpark figures (Hoffman et al., 1995). These survey data were collected in a similar fashion and should be considered non-representative.

O'Reilly & Associates are believed to be the first Internet user survey to use random digit dialing into U.S. households. They claim a sampling error of less than one percent (Frook, 1996). Their study placed over 200,000 individual phone calls and conducted 32,000 screening interviews. Ultimately, 1,000 Internet users and 500 online service subscribers were identified and interviewed for an average of 37 minutes (O'Reilly, 1996). The survey found that 5.8 million U.S. adults have direct Internet access at work, home or school, while another 3.9 million use commercial online services exclusively.

O'Reilly further projected that an additional 6 million adults will add Internet accounts or online services with Internet access by October 1996 (O'Reilly, 1996). The O'Reilly estimates are relatively low due to their restrictive definition of an Internet user. Their definition is an individual 18 or older who has direct access to the Internet, and access to e-mail and other Internet applications. The O'Reilly count excludes individuals whose only access to the Internet is through an online service (Hoffman et al., 1996).

The American Internet User Survey was conducted by Find/SVP in December 1995 . The survey was conducted by telephone to 1,000 randomly dialed Internet users. It was preceded by focus groups and a series of online surveys. The interviews included 155 in-depth questions (400 response choices) and lasted over 30 minutes each (Find/SVP, 1996). To qualify as an Internet user in the Find/SVP survey, respondents had to be current users of at least one Internet application beside e-mail. Qualified respondents included users who access the Internet form commercial online services, those who use Internet service providers, plus corporate and academic server users (Find/SVP, 1996). The survey found that 8.4 million adults aged 18 and older use the Internet, 7.4 million total users access the Web, and 1.1 million children under age 18 use the Internet. Overall, 51% of the Internet users interviewed stated they began using the Internet in 1995, confirming that the Internet audience more than doubled in 12 months prior to the survey (Find/SVP, 1996).

The CommerceNet/Nielson Internet demographic study (CNIDS) was released October 30, 1995. This was the first non-proprietary, industry-wide survey of Internet demographics. CommerceNet is a non-profit consortium of firms dedicated to promoting electronic commerce. This study was the first-ever population projectable, representative survey of who uses the Internet. Nielson Media Research was chosen to administer the survey (Hoffman et al., 1995).

CNIDS addresses three types of users in the U.S. and Canada: Internet users, online service users, and non-users. A baseline questionnaire was made up of 40 multiple-part questions, and the actual survey involved a sample of approximately 280,000 telephone calls and yielded more than 4,200 telephone based interviews (Massotto, 1995). Nielson used a random digit dial sample frame for this study. Researchers stratified the sample frame by geography to provide proportionate geographic distribution of telephone numbers. Nielson selected a systematic sample of telephone numbers to ensure equal probability. Interviews were conducted with a randomly selected member (16 years or older) of a randomly selected household. The data was weighted to reflect household differences such as multiple telephone lines. The study was designed to net approximately 1,000 completed interviews for each of the three types of users (Massotto, 1995).

CNIDS found that 37 million total persons aged 16 and above in the U.S. and Canada have access to the Internet. The study found that 24 million total persons aged 16 and above in the U.S. and Canada have used the Internet in the past three months and approximately 18 million total persons aged 16 and older in the U.S. and Canada have used the WWW in the past three months (Massotto, 1995).

The CNIDS study has been criticized by Vanderbilt University's Project 2000. This group accepted the raw data gathered by CNIDS, but performed a detailed statistical reanalysis. The Project 2000 group concluded that CNIDS survey estimates were inflated. They contend that the weighted sample was not adequately adjusted to the population it was intended to represent, and that the estimates lacked logical consistency in their definition of an Internet user (Hoffman et al., 1996). Project 2000 used the 1995 U.S. Census to reweight the raw data. They also established four Internet market segments, "Hard Core," "Regular," "Lapsed Regular," and "Infrequent," based on survey results of frequency and recency of Internet use and access. The new estimates were considerably lower than CNIDS results. Project 2000 found that 28.8 million people in the U.S. aged 16 and over have potential or actual access to the Internet, 16.4 million people use the Internet, and 11.5 million people use the WWW (Hoffman et al., 1996).

Another problem arises when attempting to count Internet users by looking at the cumulative count of the number of subscriptions to various online services. The consumer online services reached 11.3 million customers in January 1996. This represents a 78.9% increase over year end 1994 when the subscriber base for the top six online services totaled 6.3 million (Information & Interactive Services Report, 1996). The number of members reported by these services may be overstated. The online service industry encounters a phenomenon known as "churn." This describes the tendency of new subscribers to drop out soon after trying a service. Many subscribers may not be active users of a given online service, much less active Internet users (Wiggins, 1995). The percentage of online service subscribers which use the Internet is estimated at only 25% (Wiggins, 1995).

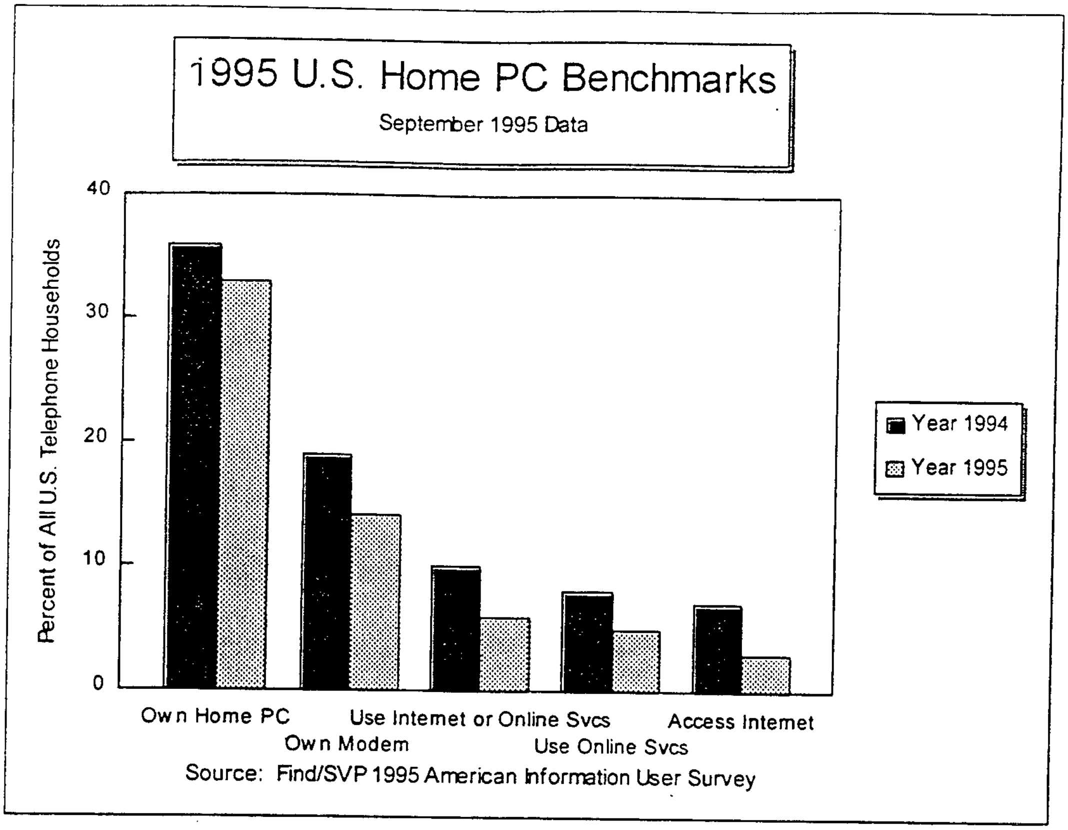
A second problem in extrapolating from the cumulative subscriber counts is the issue of duplication. Individuals may belong to more than one mass-market utility at one time. Some belong to several services. Furthermore, many people who have Internet access from their offices or schools may supplement that access by obtaining an independent service provider or subscribing to an online service (Wiggins, 1995).

C. USER DEMOGRAPHICS

The number of personal computers in U.S. homes is growing. The PC market is also "young", since 58% of PC owners have had their PCs for fewer than two years (Ziegler, 1995). Figure 7 illustrates that 36% of U.S. households own a PC, 19% of households own a modem, and 7% access the Internet (Find/SVP, 1995). Forrester Reasearch predicts that these numbers will increase to 42% of households owning a PC and 22% having an Internet connection by the year 2000 (Forrester, 1996).

The demographics of Internet users were found to be similar in all the surveys conducted. The table below shows that a majority of Internet users are male, 74% compared to 22% female.

	1995	2000
Men	6.4 million	16.5 million
Women	1.9 million	10.9 million
Children	0.3 million	5.6 million



Source: Find/SVP 1995 American Information User Survey

Figure 7: Home PC Penetration

The non-representative Hermes Internet survey found that the average age of Internet users is 32.7 years (Gupta, 1996). The age of Internet user broken down by percentage is illustrated in Figure 8 (O'Reilly, 1996). The Hermes survey found that the median income is between $50,000 and $60,000, with the average household income $63,000 (Gupta, 1996). This estimated median income is substantially higher than the national median of $36,950 as reported by the 1993 U.S. Census (Gupta, 1996). The household income of Internet users is broken down by percentage in Figure 9 (O'Reilly, 1996).

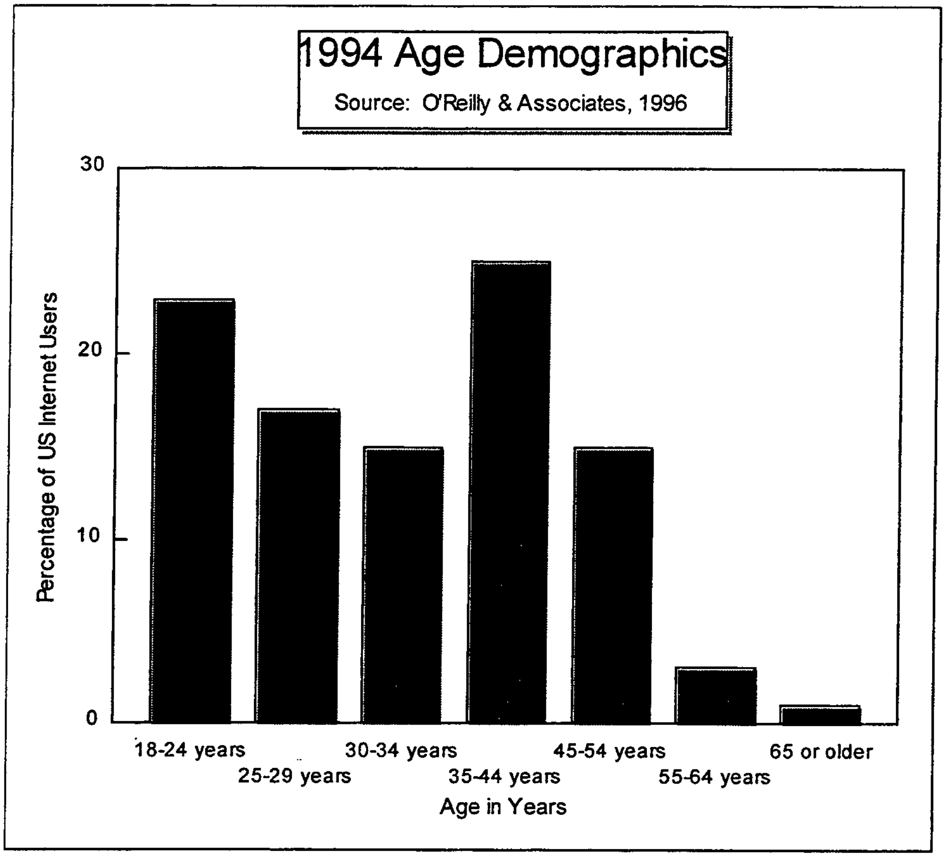


Figure 8: Age Demographics

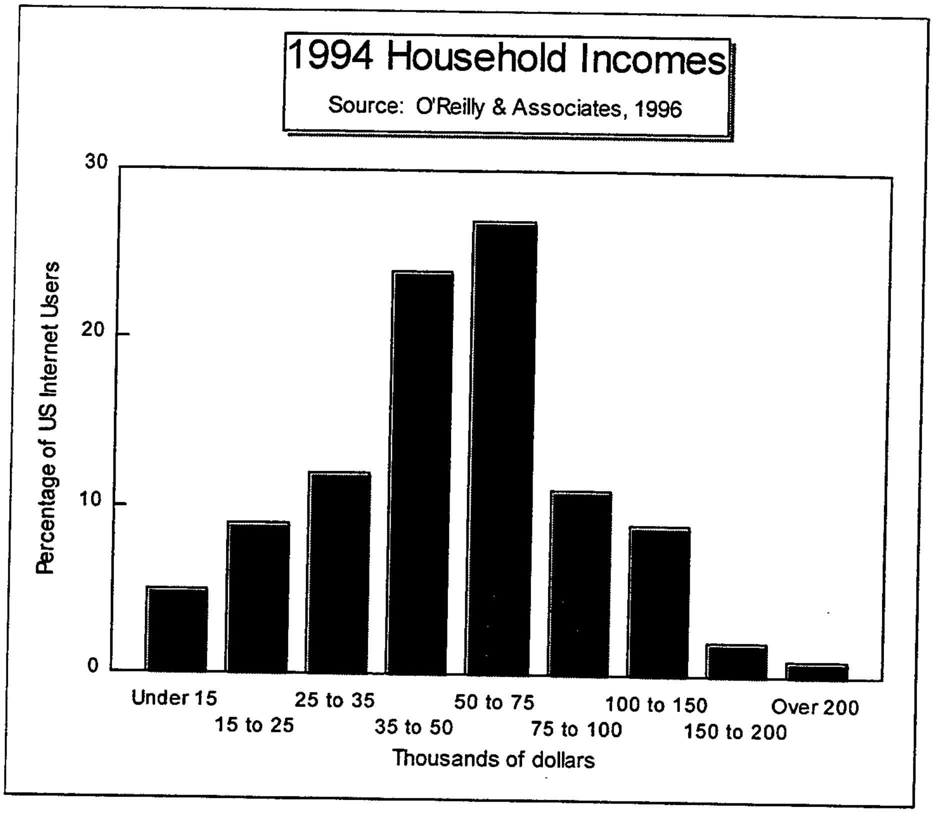


Figure 9: Income Demographics

The Hermes survey also reports that 91% of Internet users have at least some college education. (Gupta, 1995). Recent research also suggests that the demographics of Internet use are shifting over time (Gupta, 1996), the Internet appears to be moving more mainstream in its demographic profile and that this trend is likely to continue as the Internet moves toward critical mass as a commercial medium (Hoffman, 1996).

III. THE WORLD WIDE WEB AS A COMMERCIAL MEDIUM

The growth of the Internet, and particularly the World Wide Web, has led to a critical mass of consumers and firms participating in a global online marketplace. The adoption of the Internet as a commercial medium has caused firms to experiment with innovative ways of marketing to consumers in computer-mediated environments. These developments are expanding beyond the use of the Internet as a communication medium to its use as a new market (Ricciuti, 1995).

These commercial developments are occurring on the graphical interface portion of the Internet known as the World Wide Web (WWW or Web). The Web is a distributed hypermedia environment which was originally developed by the European Particle Physics Laboratory (Hoffman et al., 1995). Global hypermedia allows multimedia information to be located on a network of servers around the world which are interconnected allowing one to travel through the information by clicking on hyperlinks. Hyperlinks (text, icon, or image in a document) are able to point to any document anywhere on the Internet (Hoffman et al., 1995). The present popularity of the Web as a commercial medium results from the ability to facilitate global sharing of information and resources, and its potential to provide an efficient channel for advertising, marketing, and even direct distribution of goods and information services (Hoffman et al., 1995).

A. CONSUMER BENEFITS

The Web, as a commercial medium, offers several benefits to the consumer. The first of these benefits is the availability of information. The Web offers consumers access to greater amounts of dynamic information to support queries for consumer decision making (Hoffman et al., 1995). The Internet offers users the opportunity to overcome information chaos. Users are able to find information they really want or need in a world rife with information overload (Find/SVP, 1995). The Hermes survey of Web users found that 79% of respondents indicated that gathering purchase related information was the most preferred Web activity (Gupta, 1995).

The interactive nature of the Web allows consumers to initiate and control searches. Hence marketing communications on the Web are more consumer-driven than those provided by traditional media (Hoffman & Novak, 1995). The benefit of customer-driven searches allows consumers to become active participants in the marketing process (Hoffman et al., 1995). There is also greater probability of a consumer being well-informed, since the consumer has a greater control over the search process. Such control facilitates a highly developed form of comparison shopping (Hoffman et al., 1995).

The customer benefits from online trials. The ability of the Web to amass, analyze, and control large quantities of specialized data can enable comparison shopping and speed the process of finding items (Wallace, 1995). The Web facilitates online trials, especially in the software industry, which can provide instant gratification; customers can test products online which may prompt purchase. There is also the potential of wider availability of hard-to-find products and a wider selection of items due to the width and efficiency of the channel (Hoffman et al., 1995).

Industrial consumers realize benefits of reduced costs from increased competition in procurement as more suppliers are able to compete in an electronically open marketplace. This increase in competition leads to better quality and variety of goods through expanded markets and the ability to produced customized goods (IITA, 1994).

B. MERCHANT BENEFITS

Merchants benefit from the use of the Web as a distribution channel. The Web offers certain classes of merchants a market in which distribution costs or costs-of-sales decrease. The merchants most likely affected are those in the publishing, information services, and digital product categories (Jones, 1995). For example, digital products and software can be delivered immediately. This practice may lead to the eventual elimination of the middleman (Michalski, 1995). This may have the effect of shrinking the distribution channel, thus making the process more efficient. Overhead costs and time to complete transactions may be reduced, translating into additional efficiencies for the merchant (Kline, 1995).

The Web transfers some of the selling functions to customers. The use of online ordering and fill-out-forms gives a customer direct participation in the selling functions and bring transactions to a conclusion (Michalski, 1995). The Web is not a traditional one-way broadcasting setup like television or radio. Merchants can take advantage of this two-way channel by immediately gathering information about customers, thus providing a basis for better service.

Most merchants use the Web primarily to deliver information about the firm and its offerings (Magid, 1995). The interactive nature of the Web allows merchants to benefit by developing customer relationships. This potential for customer interaction facilitates relationship marketing and customer support to a greater degree than is possible with traditional media (Cuneo, 1995).

IDC conducted a census of Fortune 500 companies external sites on the Web since December 1995. The June 1996 report indicates that 284 companies or 57% of the Fortune 500 companies have a presence on the Web (Gens, 1996). IDC predicts this number will increase to 390 companies or nearly 80% of the Fortune 500 companies will have a presence on the Web by the end of 1996 (Gens, 1996). IDC found that 28% of the 284 Fortune 500 companies with presence on the Web offer some kind of interactive feature on their sites. IDC contends that the sites that strictly host content that is purely in the form of noninteractive electronic paper are rapidly being displaced by sites boasting interactive content (Gens, 1996). Examples of the type of interaction offered by Fortune 500 companies are:

1) Database query (65%) e.g., package tracking, flight schedules, rate quotes, catalog search, dealer locator, ATM locator

2) Financial modeling (19%) e.g., mortgage payments, college tuition savings

3) Communication (9%) e.g., opinion/content upload, customer service, virtual classroom

4) Simulation (3%) e.g., virtual tour

The interactive implementations are designed to engage customers in ongoing relationships with the firm. The merchant has two objectives in this continuous relationship-building. First, the merchant desires to provide the customer with information about the firm and its offerings. The second objective is to receive information from customers about their needs with respect to offerings. Therefore, the merchant benefits from effective customized advertising, promotion, and customer service (Berniker, 1995).

C. STATISTICS

More than 80,000 companies use the Internet for distribution of critical company information such as press releases (Roche, 1995). Nearly 14,000 firms were listed in Open Market's "Commercial Services on the Net" directory at the end of 1995. The Yahoo Business and Economic directory shows 23,540 entries under "Companies (Hoffman et al., 1995)." Although the number of companies seem impressive, O'Reilly & Associates' Online Research Group point out that the reach and acceptance of the Internet is currently limited. O'Reily researchers randomly sampled from stratified databases of North American businesses drawn from the Dun & Bradstreet database of over 7 million enterprises (O'Reilly, 1996). A total of 1030 interviews were completed. The respondents included 410 large companies (more than 1000 employees), 406 medium

(101-999), and 214 small (less than 100 employees). The survey found that 53% of medium businesses and 79% of small businesses had no Internet access and no plans to acquire one . These figures are represented graphically in Figures 10, 11, and 12 (O'Reilly, 1996).

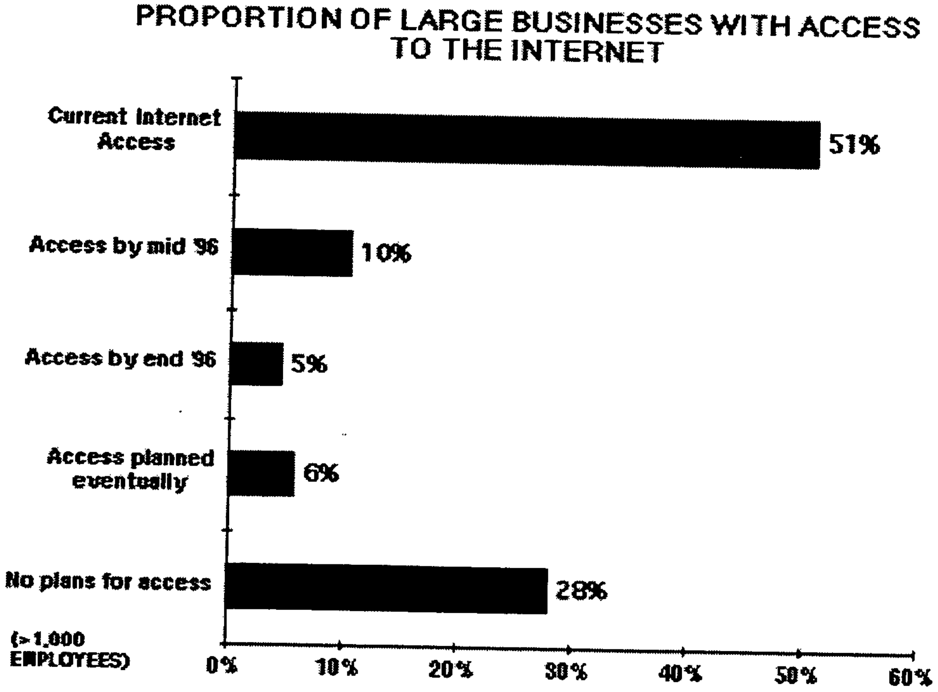


Figure 10: Large Business Access Source: O'Reilly, 1996

Don Ulsch concludes that the survey underscores the opportunity that remains for businesses on the Internet (O'Reilly, 1996). The survey found that the number of large and medium size companies online is growing. It found that 51% of large companies have Internet access, and another 15% plan to connect to the Internet by the end of 1996.

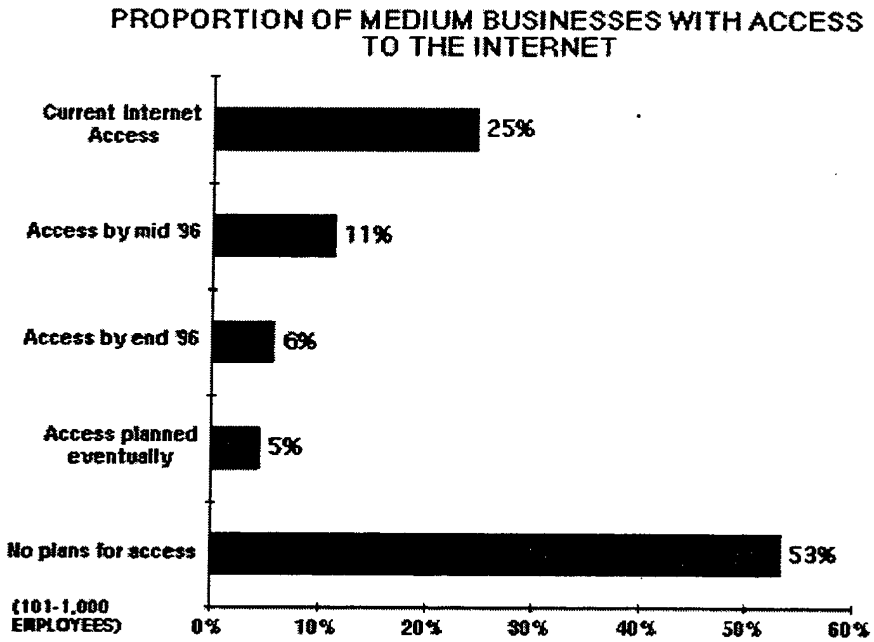


Figure 11: Medium Business Access Source: O'Reilly 1996

The survey found that 25% of medium sized companies have connected to the Internet, and 17% plan to do so by the end of 1996 (O'Reilly, 1996). The study also found that 35% of large companies and 20% of medium companies surveyed had created a publicly accessible WWW site (O'Reilly, 1996).

Forrester Research also believes that the number of companies connecting to the Internet will increase. Figure 13 shows that large (over 1000 employees), medium (100 to 999 employees), and small (20 to 99 employees) companies will all continue to grow through the year 2000 (Eichler and Modahl, 1995). The survey projects over 90% or 7500 large companies connecting to the Internet by the year 2000. Forrester predicts that

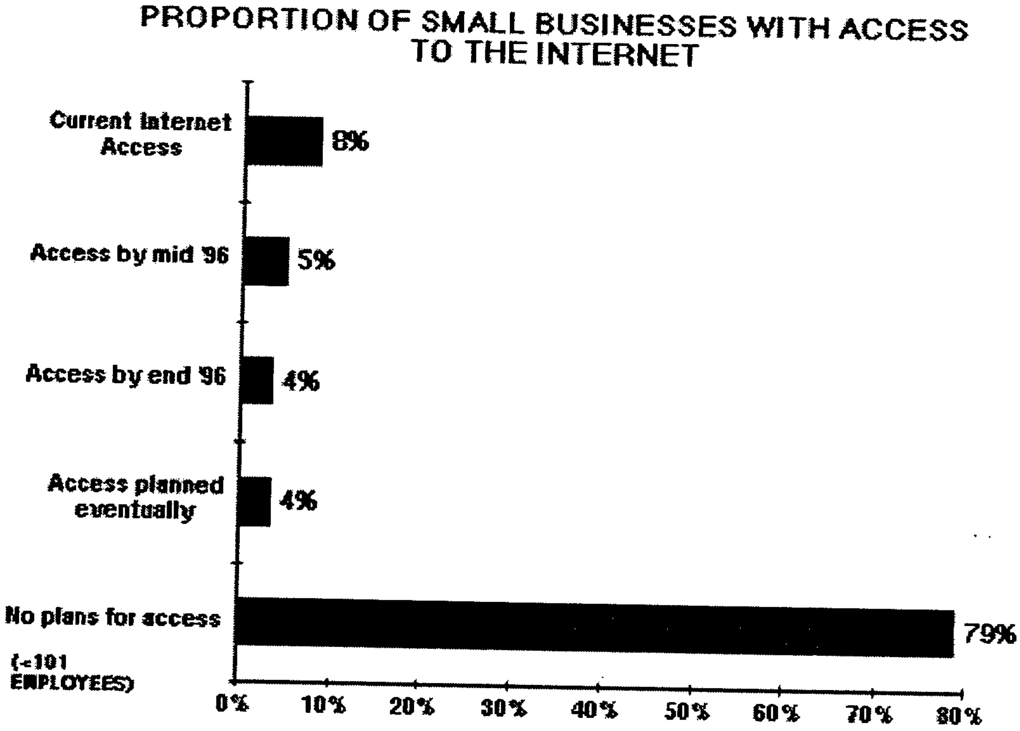
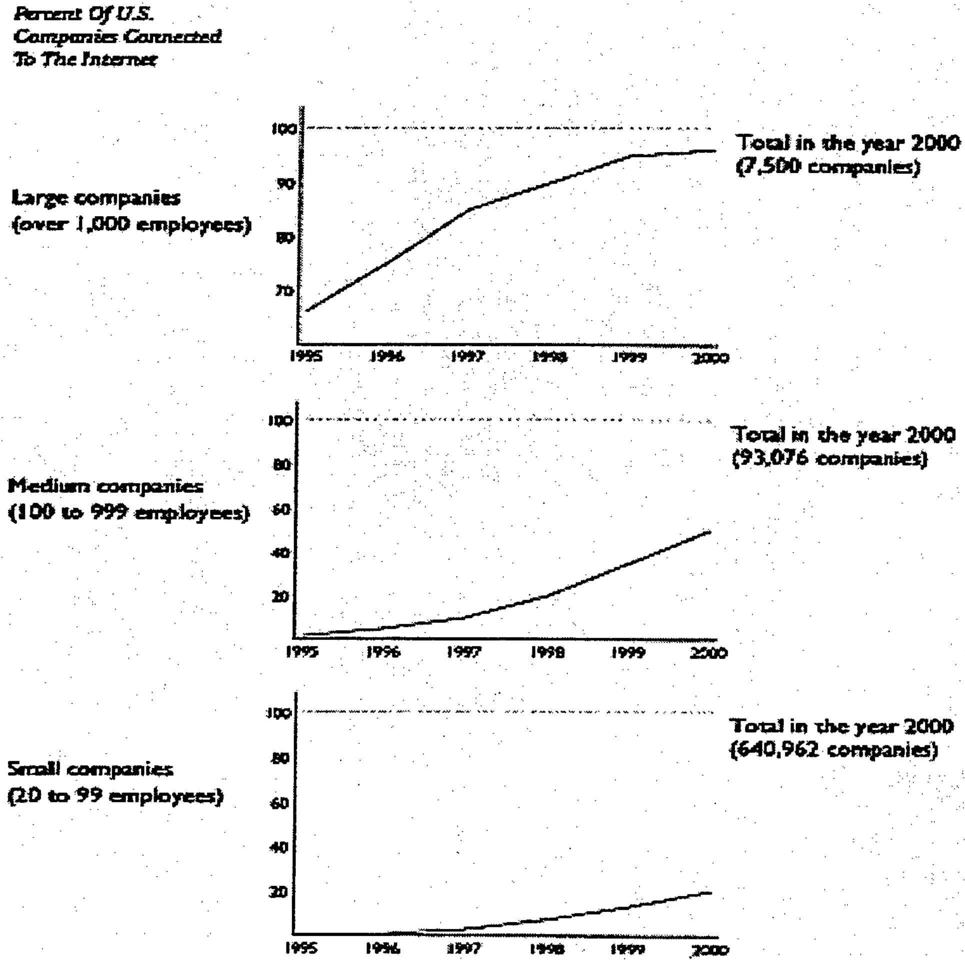


Figure 12: Small Business Access Source: O'Reilly 1996

96,076 medium companies and 640,962 small companies will connect to the Internet by the year 2000 (Eicher and Modahl, 1995). Further, ActivMedia predicts that the number of companies using the Web as a commercial medium will grow eight and a half times in 1996. They forcast an additional growth of four times in 1997 and doubling in 1998 (ActivMedia, 1996). Commercial presence on the Web may be growing, but only a small percentage of these companies currently offer consumers the ability to conduct financial transactions online. IDC found that fewer than 5% of the 284 Fortune 500 companies



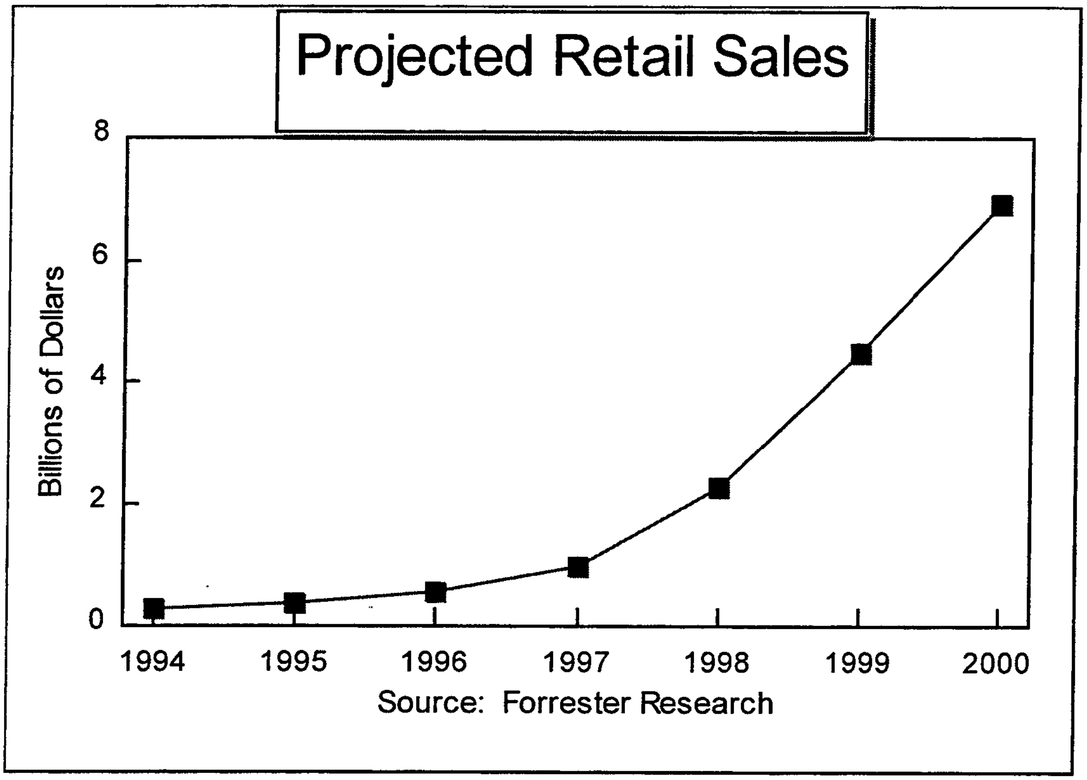
Sources: U.S. Dept. of Commerce and Forrester Research, Inc.

Figure 13: Projected Business Growth

with a Web presence offer financial transactions (Gens, 1996). However, the mere growth of companies online suggests the importance and potential of this medium. The medium contains millions of unvalued or unmeasurable interactions. The value of customer e-mail feedback, catalog requests, or five minutes online looking at a car's details will be realized off-line in the physical economy (Eicher and Modahl, 1995).

The CommerceNet/Nielson survey found that 14% of Web users have purchased products or services over the Internet. They estimate this number to be 2.5 million people (Massoto, 1995). Global Concepts conducted a survey commissioned by MasterCard International, Visa International, and Verifone Inc. which found that 32% of respondents have made purchases over the Internet (Global Concepts, 1996). The study also found that 96.1% said they were aware of online shopping, and 90.7% indicated they will likely make a purchase in the future. Global concepts surveyed over 450 Internet users. They also used focus group participants in Atlanta and San Francisco (Global Concepts, 1996).

Forrester Research estimates that $2.2 billion in revenue were directly attributable to Internet activity in 1995 (Eicher and Modahl, 1995). Forrester's market sectors include: computers, communications, publishing, retail, information services, entertainment, and financial services. The largest sector, by far, is access provided by commercial online services, with $1.5 billion in revenues during 1995 (Eicher and modahl, 1995). Forrester estimates retail sales on the Web of $350 million in 1995. Forrester predicts that retail sales will reach $6.9 billion by the year 2000. The predicted growth in retail sales is displayed in Figure 14. Forrester further predicts that total Internet-related activity will grow to $45.8 billion by the year 2000 (Eicher and Modahl, 1995). Additionally, the study found that $46.2 billion of financial assets will be managed on the Internet. Selfservice oriented customers will manage $29.9 billion of mutual fund assets and $16.3 billion in deposits online (Eicher and Modahl, 1995).



Source: Forrester Research

Figure 14: Projected Retail Sales

ActivMedia conducted a market study in 1995. The study focused on businesses generating sales on the Internet. They identified businesses with active Web sites and selected a "statistically significant and relevant research panel" (ActivMedia, 1996) by including only those companies whose products and services flowed through the Internet pipeline, and excluding those that only feed the pipeline or do not participate commercially. The study took place in two parts. An initial questionnaire was sent to

2500 marketers that matched the product category distribution of the yahoo directory, with the exception of Web consultants and Web service providers, who were excluded from the sample. The initial mailing generated 1000 responses. The second questionnaire included proprietary sales and export questions. This questionnaire was mailed to the same 2500 companies and received 231 responses. ActivMedia matched and cross tabulated the information from the two questionnaires (ActivMedia, 1996).

The study found that sales generated by the Web reached $436 million in 1995. ActivMedia predicts that sales will grow to $46 billion by 1998 (ActivMedia, 1996). The study estimates that two percent of serious Web marketers account for over half of Web sales dollars (ActivMedia, 1996). The study found that the U.S. dominates Web commerce, but that by 1998 the U.S. share is expected to fall to 70%, with increases in Canada, Asia, and Australia.

ActivMedia's study also questioned the success of Web sites. They found that nearly a quarter of the ActivMedia panel reported that they had financially successful sites (ActivMedia, 1996). Figure 15 illustrates the survey breakdown. ActivMedia reports that many of the businesses that responded to the survey had been active on the Web for less than seven months. The study found that an additional 40% of survey respondents predicted that their Web site would be profitable in 12 to 24 months (ActivMedia, 1996). The table below shows the breakdown of sales by sector. ActivMedia found that the leading Web products and services by dollar sales volume and unit sales in 1995 were as follows:

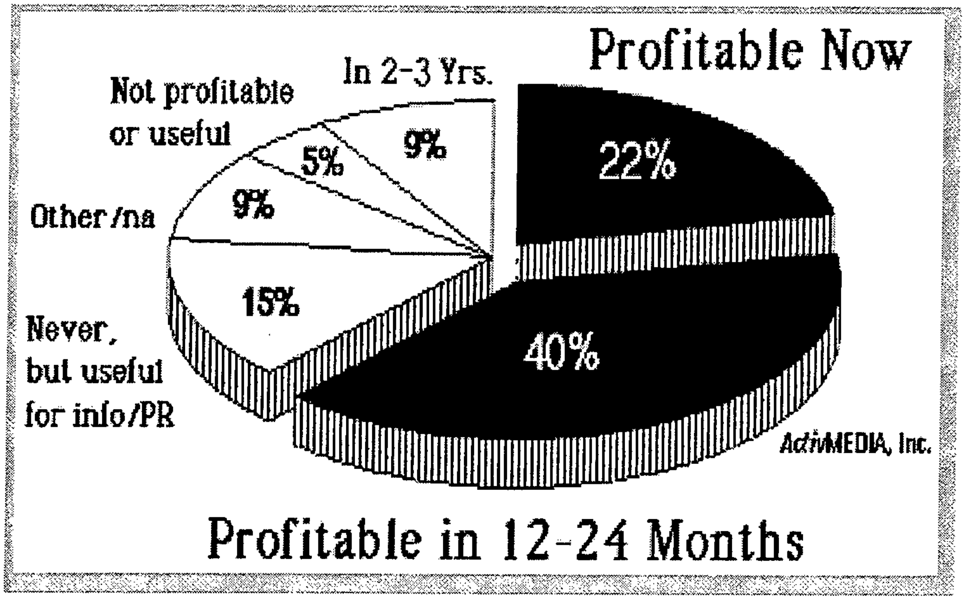


Figure 15: Profitable Businesses Source: ActivMedia 1996

Dollar Volume 1995	Unit Volume 1995
Real estate	Software
Computers and accessories	Audio/consumer electronics
Software	Computers and accessories
Travel	Other consumer products
Audio/consumer electronics	Travel
Financial services	Financial services

The preceding two surveys did not consider revenues generated by advertising when calculating Internet-related revenues. Advertising is a growing industry. ActivMedia estimates that there is nearly one Web advertising company for every seven Web marketers (ActivMedia, 1996). Advertising placement of the Web is where an advertiser pays a Web site for the privilege of displaying a banner or logo on one of the Web pages.

The banner is usually linked to the advertiser's site to generate traffic for the advertiser (WebTrack, 1996).

WebTrack conducted research to determine the size of the Internet advertising market and the major players. WebTrack examined 176 Web sites which actively solicit advertising and identified 102 which have charged advertisers in order to display their banners. WebTrack then identified the advertisers which were advertising on the Web sites and assessed the rates which they were paying (WebTrack, 1996). WebTrack was able to identify over 250 active Web advertisers with media budgets for electronic advertising ranging from $5000 to over $500,000. There were 33 advertisers who committed $100,000 or more (WebTrack, 1996).

WebTrack research indicates that fourth quarter 1995 placement expenditure totaled $12.4 million (WebTrack, 1996). The top 15 advertisers accounted for $4.2 million (34%) of the total as illustrated in the table below (WebTrack, 1996):

Big Advertisers Dominate Spending

Top 15	34%
6th to 30th largest	17%
Others*	49%

*240 advertisers

Source: (WebTrack, 1996)

The top Web advertisers in the fourth quarter 1995 are listed in the table below:

Top WWW Advertisers Q4 1995

1. AT&T	$567,000
2. Netscape	$556,000
3. Internet Shopping Network	$329,000
4. NECX Direct	$322,000
5. Mastercard	$278,000

6. American Airlines	$254,000
7. Microsoft	$240,000
8. C/net	$237,000
9. MCI	$231,000
10. SportsLine	$218,000
11. Silicon Graphics	$206,000
12. Home Arts	$201,000
13. Honda	$197,000
14. Music Boulevard	$195,000
15. Sprint	$188,000

Source: (WebTrack, 1996)

The study found that over a third of all Internet advertising is generated by other Internet providers, and more than half of the advertising is computer-related. The heaviest users of advertising services on the Internet are computer companies or others in the high-tech business (Satran, 1995).

Corporations which have popular Web sites have learned it is possible to charge thousands of dollars per month to companies wishing to place advertisements on their sites. GNN charges $7500 per week to place a pointer to a company page on its hot list (Roche, 1995). Silicon Graphics pays Hot Wired magazine $15,000 per month to have a direct link to its home page. Netscape Communications is charging $40,000 for a three-month placement on its Web site (Roche, 1995). Internet advertising is still a drop in the bucket compared with the $170 billion spent on all media (Satran, 1995). However, Alex Brown & Co. estimates it will jump to $1.4 billion by 1998 (Satran, 1995). Jupiter Communications estimates a growth to $5 billion by the year 2000. Jupiter further predicts that advertising will have established itself as the leading source of revenues on the Internet by end of 1996 (Jaffee, 1996).

IV. ELECTRONIC COMMERCE IMPEDIMENTS

A. SECURITY

Security of financial transactions on the Web is a primary concern of online buyers. The Hermes WWW user survey found that 60% of the users cite security concerns as the primary reason for not buying merchandise on the Web (Gupta, 1996). Yankelovich Partners found in another survey that 68% of online users do not feel comfortable about using their credit cards on the Web. Yankelovich Partners interviewed 400 online users and found that 90% said better Internet security is needed to ensure their personal or financial information is not accessible to unauthorized people (Jaffee, 1996). Further, the Yankelovich survey found that 79% of the respondents agreed that it is too easy for someone to steal their credit card number if they use it on the Web (Jaffee, 1996). The following table compiled from USA Today shows where users place their trust:

Where Personal Computer Users Place Their Trust	
ATM's	77%
Banking by phone	62%
Banking by computer	57%
Using credit card at a public phone	57%
Writing a credit card number on a catalog order	43%
Sending credit card data to a commercial online service	34%
Giving credit card number over phone	31%
Sending credit card number over Internet	5%

Source: (USA Today, 1995)

Credit card losses cost banks and merchants about $1.5 billion in the U.S. and $3 billion worldwide in 1995 (Lunt, 1996). MasterCard International reports that credit card fraud represents less than 9/100ths of one percent of worldwide sales volume (Lisker, 1996). The National Fraud Information Center in Washington, D.C., typically handles 350 cases of credit card fraud a day. In March 1996, 20 to 30 of these daily cases involved Internet transactions (Lunt, 1996). Forrester Research estimates that Internet commerce fraud is $1 for every $1000 worth of transactions. Comparable figures are $1.41 for credit card transactions, $16 for long-distance telephone calls, and $19.83 for cellular telephone service (Faulkner, 1996). Business Week reports that online fraud is insignificant compared to ordinary check fraud. The American Bankers Association estimates that check fraud costs banks $10 billion a year, while online fraud is running at 0.05% of check fraud or $5 million a year (Business Week, 1995).

Most retailers use a network technology called frame relay to transfer credit card information to financial institutions. Its characteristics are almost identical to the Internet network. A frame relay network is a public, packet switched, routable protocol like the Internet. The number of credit card transactions flowing across these frame relay networks dwarfs anything on the Internet. The cash register or Verifone machine actually sends your credit card information across the network twice, once to authorize the number, and once to create the final transaction (Dahl, 1995). The information is sent over the phone line at a speed of 1200 baud in clear ASCII (Busch, 1996).

The consumer is protected even if their credit card number is intercepted. In 1975, Congress passed the Fair Credit Billing Act (FCBA). Although not specifically designed for Internet related card fraud, it provides all the protection afforded conventional transactions. The maximum liability for unauthorized use of a consumer credit card is

$50. This fee is often waived by the financial institution for good customers (Grossman, 1996).

Tony Rutkowski states that Internet experts view the risk of sending a credit card number unencrypted over the Internet as no greater than giving it over the telephone. Mike Homer points out that Netscape has been conducting business online for over a year. They have had over eight million customers and not a single report of any customers' information being stolen (Grossman, 1996). Further, Forrester Research interviewed 50 electronic retailers and content providers. They found that the widespread perception of an unsafe Internet holds back electronic commerce. Interviewees said that security concerns online were a media myth. The interviewees stated that they have not experienced thieves hacking into their systems or snatching customers card numbers off the Internet. Many retailers encouraged consumers to pay online (Forrester, 1996).

B. REPORTED SECURITY BREECHES

The Federal Bureau of Investigation and Computer Security Institute conducted a survey of corporate security officers, data security officers, and senior systems analysts. The survey group sent out 4971 questionnaires and received 428 responses. The survey found that 40% of the corporate, university, and government sites that responded reported at least one unauthorized use of their computers within the last 12 months (O'Conner, 1996). Over 50% of those who experienced intrusions traced them to on-board employees. The survey found that 46.9% of users first tried patching their security breaches, while 26.6% immediately reported intrusions to law enforcement agencies. More than 16% of respondents did not report incidents (Power, 1996).

The 1995 Internet Security Survey was also conducted by the Computer Security Institute. This survey revealed that one out of every five Internet sites has suffered a security breach. The study found that nearly 40% of Internet sites do not have firewalls in place. The survey also found that 30% of security breaches occurred after a firewall was installed. The study estimates that firewall sales will grow 70% from $1.1 billion in 1995 to $16.2 billion in 2000 (CSI, 1996).

Although security breaches are rarely reported, two of the most publicized involve Netscape Communications Corporation. The first of these was a challenge issued by Netscape to decrypt a message which was encrypted using the RC4 algorithm and a 40-bit session key (See Appendix A). A French researcher working at INRIA was able to decrypt the message using a brute force attack. He used 120 workstations and two parallel supercomputers at three major research centers for eight days to break the message (Netscape, 1996). Netscape points out that the SSL protocol (Appendix A) was never compromised. Netscape estimates that $10,000 worth of computer power was used to break this single message and says that using RC4 40-bit is strong enough to protect consumer-level credit card transactions, since the cost of decrypting the message is high enough to make it not worth the computer time required to do so (Netscape, 1996).

Through reverse engineering two graduate students from the University of California at Berkeley discovered a security flaw in the Netscape Navigator browser. Goldberg and Wagner discovered that the process used by Netscape Navigator to generate random number codes was vulnerable. The two students were able to write a program that was able to predict, in a matter of minutes, session keys produced by the random number generator (Husum, 1996). Netscape Navigator uses random information to generate session encryption keys of 40 or 128-bit length (Appendix A). The random information is found through a variety of functions that look into a user's machine for information such as number of processes running, process ID numbers, and the current date and time. The vulnerability the students found exists because the size of random input is less than the size of the subsequent keys (Husum, 1996).

Netscape fixed the problem by increasing the amount of random information used to generate keys. Chatterjee explained that the key space used will increase from 30-bits to 300-bits. He also points out that the flaw did not affect the SSL protocol or encryption algorithms used by Netscape (Husum, 1996). He explains that the problem was on the implementation end of Netscape Navigator. Netscape has offered a challenge and $1,000 reward for anyone who can infiltrate the updated system. There has been no successful attempt (Lynch, 1996).

Citibank was victim of the first reported case of electronic bank fraud in the United States. Vladimir Levin, a 28 year old mathematics graduate working for a trading company in St. Petersburg, Russia, was able to penetrate Citibank's cash management system over 40 times in five months (Times of London, 1995). According to the FBI, Levin obtained $400,000 from the accounts of three banks, two Argentinean and one Indonesian. Citibank's cash management system allows Citibank customers to initiate their own funds transfers to other banks; daily turnover is about $500 billion (Flohr, 1995). A further $11.6 million was illegally transferred after Citibank called in the FBI, who asked that the transfers be allowed to take place so they could trace the hackers. The money was transferred to accounts held by a Russian in California and to other Russian-held bank accounts in six other countries, including Israel, Germany, Holland, and Switzerland. Citibank officials say only the first $400,000 was lost. Levin was apprehended at Stansted airport in England after leaving St. Petersburg (Times of London, 1995).

Citibank uses IRE security products. Seven of the ten largest banks in the U.S. also use IRE products. The company has supplied encryption devices to the U.S. National Security Agency, Federal Bureau of Investigation, and the U.S. Department of the Treasury. Leukhardt explains that Citibank made the use of strong security measures optional for customers and that Levin and his accomplices exploited the fact that some end-users were only using conventional I.D.'s and passwords (EDI News, 1996).

Kevin Mitnick is a 31 year old computer programmer who had been on the run since 1992 for violation of a prior computer fraud probation order. Mitnick was arrested in Raleigh, North Carolina on February 15, 1995 for computer fraud. He had allegedly pilfered thousands of data files and at least 20,000 credit card numbers from Netcom Communications, an Internet service provider based in San Jose, California (NY Times, 1995). This is the sixth time Kevin Mitnick was arrested for computer fraud. It took the efforts of security expert Tsutomu Shimomura, MCI, Sprint, Netcom Communications, and the FBI to apprehend Mitnick (NY Times, 1995). Mitnick has been awaiting trial for over 18 months while awaiting the conclusion of FBI investigations. He has only been charged with cellular telephone fraud and a probation violation. There has been no accusation of credit card fraud (Stone, 1996).

C. CUSTOMER INTERFACE BARRIERS

Roy Bunyan of ICL Financial Services claims that the risk of fraud is not the main obstacle to the progress of commerce on the Internet. He says that a lot of money is being spent on security, when the real barriers are access and speed. Bunyan says that it takes longer to perform comparative shopping on the Internet than it does to pick up the telephone and order the same item in a catalog (Wilson, 1996). He claims that as the Internet grows the problem will get worse. Bunyan says that the future lies in developing smart browsers which understand shopping habits and learn constantly. He believes this will enable less data input for the consumer each time they shop, leading to a more efficient shopping experience (Wilson, 1996). Bunyan envisions a smart agent or third party broker who will search the Web for your product input and provide the product information requested (Wilson, 1996).

Hoffman agrees that online dynamic content directories must be developed to keep pace with the growing Web. She feels that efficient ways to help consumers sort and search through the vast offerings will be critical (Hoffman et al., 1996). Research in consumer decision making suggests that decision effectiveness degrades in the presence of too much information (Hoffman et al., 1996). Therefore, the challenge for marketers will be to develop, in conjunction with consumers, rule-based systems for the organization of content that exploit the principles of network navigation and facilitate flow (Hoffman et al., 1996).

The organization of the Web site itself can be critical. The Hermes survey found that the most widely cited problem with using the Web was that it takes too long to view/download pages (69.1%). This problem is supported by the finding that 33.7% of the users report using 14.4 kbs modem and 26.6% use a 28.8 kbs modem (Gupta, 1996). ActivMedia's survey also found that Web sites with expensive graphics often restrict sales. They found that these sites attract a lot of users who not only do not buy, but also interfere with real buyer's access and the company's ability to serve those buyers (ActivMedia, 1995). Further, the Hermes survey found that 34.5% of users were unable to find a Web page they knew exists. Other problem areas identified by users was 25.8% not being able to organize the pages and information they gather and 23.7% not being able to find a page once visited (Gupta, 1996).

Another barrier to electronic commerce is a lack of Web sites that offer transactions online. A recent study of Fortune 500 companies found that while nearly 80% of the companies are expected to have a Web presence by the end of 1996, less than 5% of these offer core business transactions online (Gens, 1996). IDC believes that although a relatively small number of companies offer core business transactions, the early adopters will quickly drive competitors to follow suit (Gens, 1996).

Lack of sites that consumers view as superior to the conventional marketing channels is holding back the Web. The Web needs sites which deliver exceptional value to consumers and make it convenient for finding and buying goods (Chen, 1996). Broadvision (See Chapter 6) feels that one-to-one marketing is the answer. The driving principle of one-to-one marketing is getting to know your customer better. A collaborative dialogue is established. The objective is owning a piece of the customer's mindshare and providing personalized services addressable to each customer according to their preferences (Broadvision, 1996). The company can then forge long-term relationships with loyal customers, responding to and even anticipating their personalized needs (Chen, 1996). Once the customer is known, the company can track their patterns of activity over time. This idea is not new, but what is different is the ability to tailor a message to the consumer while they are connected online, engaged in a live two-way medium. Chen says that the once the dialogue starts, the software will learn by observing consumer choices and subsequently provide more focused information, entertainment, and transactional capabilities to the individual consumer. Chen believes it is the capacity to learn, remember, and personalize that will draw consumers back to a Web site (Chen, 1996).

D. COSTS TO BUSINESSES

Startup costs to businesses can be an impediment regardless of the projected rate of return advertised. Terry Fletcher estimates the startup cost of advertising on someone else's Web site to be nearly $6000. He estimates $2800 for development of layout, concept, and model page, $400 for analysis of competitors, $400 for programming of the Web page, $650 for programming of interactive forms, $975 for graphics, $810 for submitting pages to various Internet yellow pages, and $200 for updates per page per time (Fletcher, 1996). Fletcher estimates the startup costs for developing a commercial site to be $100,000. He figures a minimum of four machines are needed (Web server, file server, news server, and mail server), but ten machines are preferred to handle user load. He quotes the Sun or Hewlett Packard workstations at $5000 plus an additional $5000 for a binary license for each machine. Fletcher estimates annual disbursements to be

$78,000. The disbursements are broken down as follows: $2000 monthly for unlimited traffic volume, $1000 per month for the T1 net connection, $500 per month for telephone lines, and $300 per month utility bill for each workstation, monitor, and printer (Fletcher, 1996).

International Data Corporation surveyed medium to large-sized corporations maintaining the largest and most sophisticated interactive commerce channels on the Web. The study of corporate Internet application development discovered that the cost of establishing an interactive commerce business channel is four times greater than expected, and twice as much time is spent on customizing sites as anticipated (Connect, 1996). The study revealed that while 20% of Web site development costs are spent on hardware and off-the-shelf software, 80% is spent on custom software development and integration (Connect, 1996). Respondents indicated they spent from $840,000 per site with minimal security, to more than $1.5 million for highly-secured sites (Connect, 1996). ActivMedia estimated Web site development expenditures at $116.3 million and Web storage payments to external providers at $15.1 million for 1995 (ActivMedia, 1996).

V. PROTOCOLS

A. ANONYMOUS CREDIT CARDS / INTERNET MERCANTILE PROTOCOL

Introduction

Electronic communications networks bring consumers, merchants and financial institutions together and provide for electronic commerce transactions. The objective, however of anonymous credit cards and anonymous internet mercantile protocol (AIMP) is to keep information apart to protect personal privacy. AT&T Bell Laboratories have proposed a simple standard cryptographic system to accomplish this task. The credit card application separates the consumer's identity and purchases in order to protect that individual's privacy. Information delivery returned to the customer is also kept anonymous (Kristol, 1994). The organization that extends credit needs to know a person's identity and the store knows the purchases, but no single entity knows both (Low, 1994). Therefore, the organization extending the credit does not have access to specific purchases, and the merchant is paid without knowing the consumer's identity.

Functionality

The credit card company uses a different bank to set up an anonymous account, which the individual uses when purchasing. As a purchase is being made, funds are transferred from the anonymous account to the merchant's account. The only distinction between anonymous credit cards and AIMP is that AIMP can be used on the Internet to perform anonymous funds transfer (Kristol, 1994).

Other credit card company functions need to continue as users expect an itemized billing statement to be able to challenge purchases, and to be notified if their card is being used in an unusual manner. These responsibilities remain with the credit card company.

Double-locked Box

A double-locked box protocol is used to transfer funds between accounts in order to make the system more difficult to break (Low, 1994). An intermediary known as a communications exchange (cx) acts as an electronic Federal Reserve to settle accounts among banks and to log messages to create an audit trail. The intermediary is used to conceal information so that neither bank knows the identity of the other, and only the bank maintaining the anonymous account knows the transactions occurring. The user deposits a box in the source account that can only be opened by the intermediary. Inside this box is the name of the destination bank, and a second box that can only be opened by that bank. The second box contains the name of the account (Low, 1994).

Cryptographic Tools and Protocol Specifications

Cryptographic Tools

Public key cryptography is used for encryption and digital signatures (Appendix A). Each player in the system maintains a public and private key. The public key is known but the private key is only known by its owner. Authentication of each player is accomplished via digital signature as the transaction message arrives at a destination. The message consists of a time stamp sent in the clear, followed by a function of the message and the time stamp encrypted with the private key of the player (Low, 1994).

Protocol Specifications

The protocol achieves three objectives (Kristol, 1994):

(1) The seller's interest is protected by transferring funds to the seller's account before information/merchandise delivery. Furthermore, the information is encrypted so that it is useless to all but the paying customer.

(2) The customer's anonymity is guaranteed by the use of information separation and cryptographic techniques.

(3) The customer's interest is protected by the creation of a complete (but encrypted) audit trail that can be unraveled when necessary to settle any dispute.

The protocol has three distinct steps (Low, 1994):

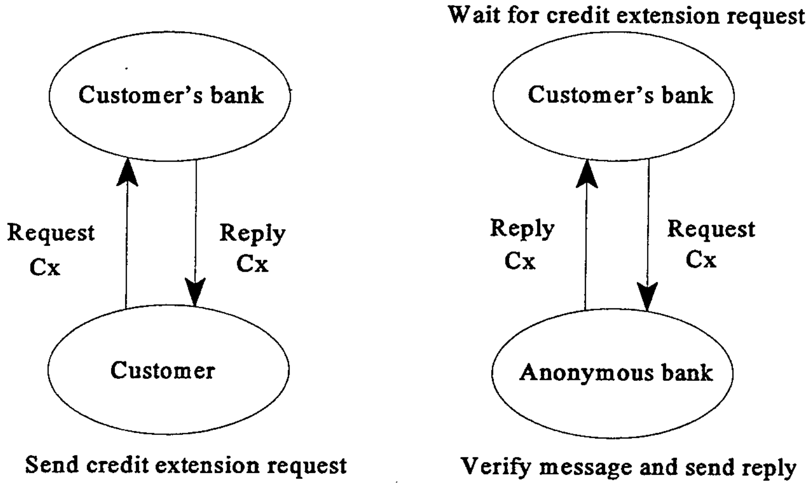

Wait for credit extension request
Customer's bank
Request Cx
Reply Cx
Customer
Send credit extension request
Customer's bank
Reply Cx
Request Cx
Anonymous bank
Verify message and send reply

Figure 16: Extension of Credit

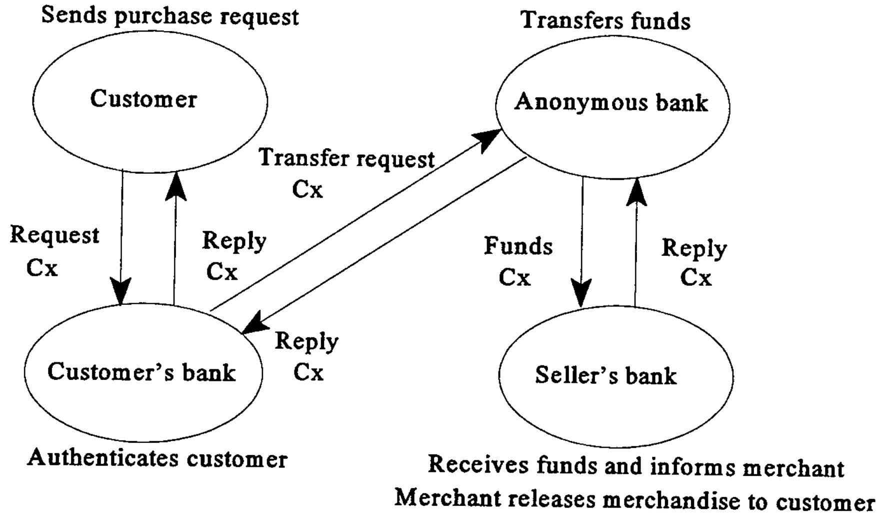


Figure 17: Purchase Transaction

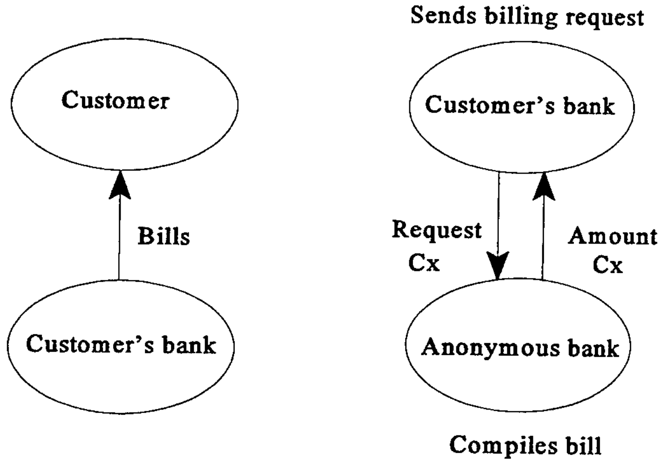


Figure 18: Transfer of Billing Information

Collusion

Collusion is the combining of information using the communications exchange (cx) in order to perform financial electronic transactions. When two parties have a common, unique piece of information, they can combine their information (Low, 1994). The ability to extract information by collusion may make funds transfer mechanism more acceptable as anonymous accounts are currently illegal in the United States and there is concern about anonymous mechanisms being used for illegal reasons (Low, 1994). Collusion can be forced as sort of an "electronic equivalent of a subpoena" to determine a person's identity and purchases. The number of different parties that must collude to associate a person's identity and purchases is five. No single player has enough information to link customers to merchandise (Low, 1994).

Conclusion

Computing and data storage are becoming less expensive paralleling an increased use of credit and debit cards (Low, 1994). This allows profiles of consumers to be assembled and sold. Therefore it is possible to determine how much alcohol or tobacco you purchase or even which videos you rent with this information being readily available. Cash solves the problem only if you are not reluctant to carry it at all times. This protocol allows people to preserve their privacy in the conventional market place and on the Internet without losing the advantages associated with credit cards. The disadvantage is that fees are required to maintain an anonymous bank account and the communication exchange (intermediary). The anonymous credit card and AIMP protocol applications are in the development process and not yet available.

B. FIRST VIRTUAL GREEN COMMERCE MODEL

Introduction

The green commerce model proposed by First Virtual Holdings requires an Internet user to establish a cardholder account which is associated with a user's bankcard or checking account. The cardholder account is identified by a 12 digit alphanumeric string (First Virtual PIN assigned by FV) which is unique to a particular user (Gable, 1996). No bankcard or checking account numbers are used. The First Virtual system (green commerce server located in Austin, Texas) confirms each transaction and initiates settlement off-line through a conventional, secure link to processing agents, banks and credit cards (Gable, 1996). The green commerce server maintains all cardholder accounts and is responsible for funds transfer. Cardholder FV PINs (card numbers) are stored unencrypted in a separate computer system (FV customer service telcon 1996).

Associated with each cardholder account is (Stein, 1995):

(1) Internet electronic mail address

(2) State (active, seller-only, suspended or invalid)

(3) Pay-in method (i.e. bankcard)

(4) Pay-out method (i.e. direct deposit into a checking account)

(5) Type of currency (i.e. U.S., Canadian)

The cards are bi-directional. A cardholder may engage in commerce as both a buyer or a merchant. The terms buyer and merchant only indicate the direction of the funds transfer for a transaction (Stein, 1995).

Green Commerce Model Transactions

The green commerce model provides cardholders with eight possible transactions. The transactions are exchanges of messages between cardholders and the green commerce server (Stein, 1995).

1. Funds Transfer

The transaction occurs when one cardholder (merchant) requests funds from another cardholder (buyer). The buyer initiates a purchase using their card number (FV PIN). A transfer request message is sent to the green commerce server. The message contains the merchant and buyer card numbers, the transfer type (sale of information), and the transfer amount and currency ($1.00 U.S.). The green commerce server sends a transfer query message to the electronic mail address associated with the buyer's account (Stein, 1995). The transfer query message contains a transaction identifier uniquely generated by the server, the merchant and buyer names, the transfer type, and amount and currency associated with the buyer's account. The green commerce server waits for a response. If there is no response after a pre-determined number of days or number of transfer query messages are exceeded, the buyer's card number enters a suspended state. The card number will return to an active state once the number of transfer query messages for the buyer drops to less than a certain threshold.

The buyer sends a transfer response message. The transfer response message contains the server's transaction identifier and the buyer's response (yes, no, or fraud). The green commerce server sends a transfer result message to the merchant's electronic mail address associated with the merchant's account. The transfer result message contains the server's transaction identifier, the merchant and buyer names, the transfer type, and the buyer's permission to transfer the amount in the currency associated with the buyer's account. If the buyer indicated "yes", then the transaction is added to the green commerce server's settlement queue for the buyer. If the buyer indicated "no", then a service charge may be added to the green commerce server's settlement queue for the buyer. If the buyer indicates "fraud", then the associated card number enters the invalid state (Stein, 1995).

The green commerce server periodically checks the settlement queue for each cardholder. A batch of accumulated transactions will be placed into a conventional, secure transaction every 91 days using the pay-in/pay-out method associated with the cardholder's account (FV customer service telcon, 1996). If the pay-in/pay-out method fails, then the card number enters a suspended state and the green commerce server sends a pay-in/pay-out failure notification message to the associated electronic mail address. The pay-in/pay-out failure message contains the server's transaction identifier and the amount and currency associated with the transaction. If the funds transfer succeeds, the green commerce server sends a pay-in/pay-out notification message to the associated electronic mail address. The pay-in/pay-out message contains the cardholder's name, the pay-in/pay-out amount and currency type, the list of accumulated transactions and a service charge if applicable (Stein, 1995).

2. *Card Number Inquiries*

The card number inquiry transaction occurs when one cardholder wishes to obtain the state of another cardholder's account. A cardholder acting as a merchant may inquire when considering a sale to another cardholder. The merchant sends an inquiry request message containing the buyer card number to the green commerce server. The green commerce server replies with an inquiry result message containing the buyer card number and the state associated with the cardholder's account to the electronic mail address of the merchant (Stein, 1995).

3. Transfer Inquiries

The transfer inquiry transaction occurs when a cardholder wishes to obtain the status of a funds transfer. Typically a merchant wants to find out the last action taken by the green commerce server. The merchant sends a status request message containing the merchant's card number and the transaction identification number to the green commerce server. The green commerce server replies with a status result message containing the merchant's card number and information about the last message sent by the green commerce server with respect to this transaction. The result message will indicate that it is either waiting for a transfer response message or the transaction has been placed into the settlement queue (Stein, 1995).

4. Chargebacks

The chargeback transaction occurs when a real-world funds transfer associated with a previous pay-in notification message results in a chargeback. A cardholder using a bankcard disputes a charge from the green commerce server after the server generates a real-world transaction. The green commerce server sends a pay-in chargeback notification containing the notification identifier associated with the pay-in method, the pay-in amount, and currency type to the associated electronic mail address. A pay-out chargeback notification is also sent to the merchant's electronic mail address with the same information (Stein, 1995).

5. Server Capabilities

The server capabilities transaction occurs when a cardholder inquires about the capabilities of the green commerce server. The cardholder sends a capabilities request message containing the card number to the green commerce server. The green commerce server replies with a capabilities result message containing a list of supported transaction types (funds transfer, card number inquiries, transfer inquiries, chargebacks, server capabilities, cardholder applications, account maintenance, and account history) and a list of supported currencies (Stein, 1995).

6. Cardholder Applications

The cardholder applications transaction occurs when an Internet user applies for the green commerce cardholder account. The applicant sends an application request message via electronic mail to the green commerce server. The green commerce server sends an application result message containing a set of cardholder parameters to be filled in by the user. The user fills in the required information and sends the request back to the green commerce server. The green commerce server replies with a new account result message containing the status of the application and the card number assigned to the applicant (Stein, 1995).

7. Account Maintenance

The account maintenance transaction occurs when a cardholder wants to change account information. The cardholder sends a change request message containing the card number to the green commerce server. The green commerce server replies with a change result message containing the card number and information to be filled in by the user. The cardholder fills in the information and sends a change account request message to the green commerce server. The green commerce server sends a change account query message containing a transaction identifier uniquely generated by the server and a list of attributes to be changed to the associated electronic mail address. The green commerce server waits for a response. If the cardholder responds, then a change account message containing the server's transaction identifier and the cardholder's response (yes, no or fraud) is sent to the green commerce server. If the cardholder indicated "yes", then the green commerce server sends a change account result message containing the server's transaction identifier and a list of attributes to be changed to the associated electronic mail address. If the cardholder indicated "no", then no action is taken. If the cardholder indicated "fraud" then the cardholder's card number enters the invalid state (Stein, 1995).

8. *Account History*

The account history transaction occurs when a cardholder wants a history of message activity. The cardholder sends a history request message containing the associated card number to the green commerce server. The green commerce server responds by sending a "multipart/mixed" message containing recent messages sent to the cardholder by the green commerce server to the associated electronic mail address (Stein, 1995).

Conclusion

The merchant carries all risk of non-payment. The key security issue surrounds the transfer response message sent by the cardholder acting in the buyer role. The transfer response message contains the uniquely generated transaction identifier in the transfer query message which is sent to the cardholder acting in the buyer role. The transaction identifier does increase security. However, it does not minimize the likelihood that electronic mail is intercepted. Electronic mail can be intercepted if a sniffer program is used to search for key words. Merchants selling goods instead of information are discouraged from using First Virtual because payment is not received until 91 days after the transaction (FV customer service telcon, 1996). First Virtual uses this tactic to deter chargebacks since purchases after three months increase customer expense (FV customer service telcon, 1996). Cryptographic applications would provide protection from interception and manipulation of the transfer response message. There are several secure e-mail applications for added security: PEM, S-MIME (RSA), PGP.

Advantages of First Virtual Green Commerce Model:

(1) Simple

(2) Off-line conventional financial transactions

Disadvantages:

(1) Buying through e-mail message which can be intercepted and manipulated.

(2) Transaction identification can be intercepted and manipulated.

(3) Slow: No advantage of instantaneous transaction for the compulsive buyer.

(4) Payment does not reach a merchant's account for 91 days.

C. GSS-API FOR WEB SECURITY

Introduction

Generic Security Service Application Program Interface (GSS-API) is under development by the Internet Engineering Task Force Common Authentication Technology Working Group. The IETF goal is to provide a standard programming interface that Web applications can use to secure transactions over the Internet (Rosenthal, 1995). As with Secure Sockets Layer (SSL), the GSS-API can be used to secure other applications in addition to the Web (Netscape, 1996).

Web Functionality and Integration

IETF is defining a negotiation protocol to enable GSS-API -based applications to negotiate and select common security mechanisms at run-time (Rosenthal, 1995). The protocol will provide for the interoperability of Web applications across a variety of security environments by allowing a Web client and server to support GSS-API mechanisms. The GSS-API can be incorporated into a variety of client/server application protocols (including HTTP). The integration occurs at the network communications level providing security for various types of HTTP transactions (Rosenthal, 1995).

The definition of a new secure HTTP URL type is part of the Web/GSS-API integration. The URL type demonstrates that the Web data must be accessed using a GSS-API mechanism. A chosen security method must be used to enable the client to secure its request to the server. GSS-API implementations that support GSS-API mechanism negotiation, a common security mechanism type and mechanism options are selected via the mechanism negotiation protocol (Rosenthal, 1995). A security context using the selected mechanism is established. Web applications that only support a single GSS-API mechanism default to the common security program between the client and the server. It also goes to the common security program if an error is returned in the negotiation process (Rosenthal, 1995).

Acquiring Credentials and Security Context Establishment

Credentials are required for security context establishment. Acquiring credentials makes available the relevant credential data for the client and server to be authenticated via the subsequent context establishment (Rosenthal, 1995). Credentials have a useful life and can be re-used until expiration. When credentials expire, they must be re-acquired. Clients and servers may have different expirations depending upon the level of security. The acquisition process is varied depending upon the GSS-API mechanism being used. One or more mechanism-specific (non GSS-API) functions must typically be called prior to acquiring credentials (Rosenthal, 1995). Rosenthal provides example credential data:

(1) Kerberos tickets

(2) Private/Public Key Pairs

(3) Public Key Certificates

The process of security context establishment provides for authentication of the client and the server and establishes a secret key for Web transaction protection. The Web client initiates the security context, and the Web server accepts the security context (Rosenthal, 1995).

Initiating and Accepting a Security Context

The Web client initiates a security context using the GSS_Init_sec_context() function, passing the following as input arguments (Rosenthal, 1995):

(1) The credentials (public/private certificates) returned from GSS_Acquire_cred(), or

null to use default credentials.

(2) The name of the server.

(3) A security mechanism type (selected during the negotiation process).

(4) A set of context-quality flags (indicate the quality parameters associated with the security context as conveyed by the client).

The server name is used by the underlying GSS-API mechanism to obtain the appropriate server credential information needed to authenticate the client with the server (Rosenthal, 1995). Additional information is required to interpret the URL in environments where multiple authentications exist. If mechanism negotiation is supported, the mutual/anonymous authentication procedures are set as per the mechanism type and mechanism options selected during the mechanism negotiation phase (Rosenthal, 1995). If the server is configured for authentication, then mutual authentication will be required during the mechanism negotiation process. Mutual authentication is not required when the server is not configured for authentication.

The Web server accepts a security context using the accept security context function, passing the following as input arguments (Rosenthal, 1995):

(1) The credential handle returned from the acquire credential function, or null to use default credentials.

(2) The context token received from the client.

If successful, the accept security context function returns the following as output arguments (Rosenthal, 1995):

(1) The name of the client user.

(2) A set of context-quality flags.

(3) Message protection service flags (indicate whether message confidentiality and/or integrity services are available for the context).

The returned client name represents the authenticated identity of the user. The external representation of the authenticated user name can be used to enforce access controls on client requests (Rosenthal, 1995). If acceptance does not occur, the server disconnects from the client.

Message Protection

GSS-API functions are used to exchange information between the Web client and server in a secure manner once the security context is established. Transactions can be secured by a Message Integrity Code (MIC) alone, or by a MIC with public key encryption (Appendix A) of the transaction data (Rosenthal, 1995). Digital signatures can be used to ensure the integrity of the entire transaction.

After the security context is established, the server enforces the level of security required for a transaction and sends the client a message that is secured at that enforced level. The server indicates to the client whether integrity alone or integrity with encryption is required and which integrity/encryption algorithm(s) must be used. The server also indicates the key size to be used for encryption (Rosenthal, 1995). The security level and type that is indicated by the server must agree with that supported by the GSS-API mechanism being used. If the mechanism support is not present, or the message transactions are not protected in the same manner as was originally indicated by the server, the server disconnects from the client (Rosenthal, 1995).

Conclusion

Generic Security Service Application Program Interface (GSS-API) does not define a network or a wire protocol. However, it can be used for securing financial transactions over the internet in accordance with the IETF requirements for Web security. GSS-API enables client and server authentication and data encryption capabilities to be incorporated into Web browsers in a secure and independent manner. GSS-API provides a generic programming interface which can be layered above different security mechanisms. The programming interface provides security services supporting a range of underlying mechanisms and technologies in different security environments (Linn, 1996). This is a move by IETF to standardize and promote both electronic commerce and open systems.

D. IBM INTERNET KEYED PAYMENT PROTOCOLS (iKP)

Introduction

IBM Research Division has developed a family of secure multi-party payment protocols called Internet Keyed Payment Protocols (iKP). Designed to work on any browser, iKP technology (based on RSA public-key cryptography) allows customers to order goods, services, or information over the Internet, while relying on existing credit card or ATM networks to implement the necessary payments (Wayner, 1996). iKP electronic payment transaction may involve one, two, or three public keys. The bank acquiring the transaction for processing will have a public-private key pair for receiving confidential information (credit card numbers and signing authorization messages).

iKP Protocol Participants

The iKP protocols are designed to allow buyers to order goods, services, or information over the Internet while relying on existing secure financial networks to implement the necessary payments. The iKP protocol provides complete cryptographic protection and a solid audit trail that can be used to resolve any disputes (Wayner, 1996). Participants in the iKP protocol are (Linehan, 1995):

(1) Buyer and Seller

(2) Seller's Bank and Buyer's Bank

The seller's bank functions as a gateway between the internet and existing financial networks that support transactions between banks. The seller's bank maps the iKP protocol conducted on the Internet to the protocols used on the financial networks. iKP requires no changes in the communication between the buyer's bank and the seller's bank. Secure financial networks already exist to connect financial institutions (banks) therefore, iKP is not concerned with bank security issues. iKP is specifically designed to address security issues that arise in buyer and seller communications.

iKP Protocol Description

iKP may be used with a variety of communications channels (ie. SSL, HTTP, SHTTP, electronic mail). The general architecture accommodates a variety of payment methods by making certain message flows and fields optional. Prior to any iKP transaction, the buyer and seller must have already agreed on the details of the purchase order, the price and currency, and the payment method. Three iKP protocol scenarios exist and represent different levels of security (Wayner, 1996):

The lowest level, 1KP, requires that a central authority publish a certificate guaranteeing its public key (Appendix A). A large scale public key infrastructure is not required since public key certificates do not need to be issued to everyone. The customer making a purchase encrypts the credit card number, the expiration date, and a secure hash of the information about price and details of the transaction. The merchant then adds its own secure hash of the transaction details to the customer encrypted information. The bank decrypts the customer's information and verifies both the customer's hash and the merchant's hash. Once verified, the bank signs this approval or rejection and the secure hash of the transaction details with its own digital signature. The customer and the merchant can also verify the bank's digital signature (Wayner, 1996).

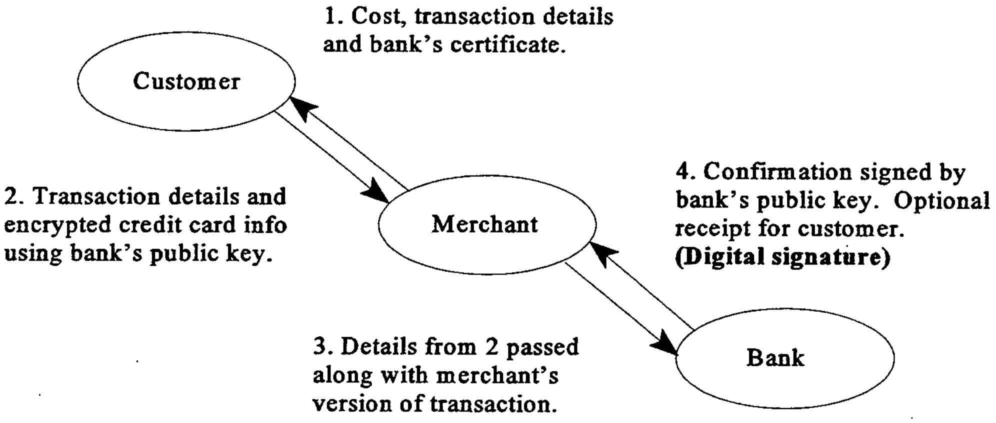

1. Cost, transaction details and bank's certificate.
Customer
2. Transaction details and encrypted credit card info using bank's public key.
Merchant
4. Confirmation signed by bank's public key. Optional receipt for customer. (Digital signature)
3. Details from 2 passed along with merchant's version of transaction.
Bank

Figure 19: 1KP Protocol

The next level requires each merchant to publish a public key that is certified by a central authority (Appendix A). Each merchant uses a certified public key pair and adds its signature to the packet containing the customer's encrypted transaction details. The customer can verify this certificate and know that the merchant is approved by the bank (Wayner, 1996).

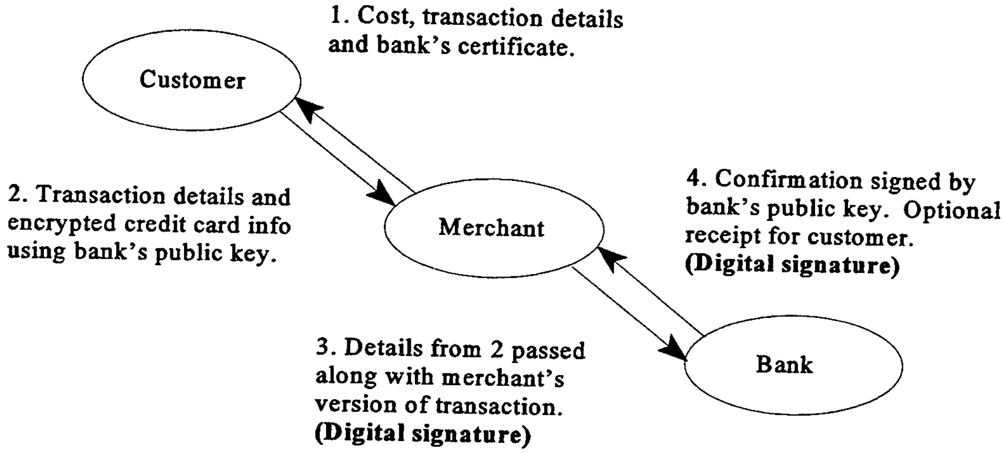

1. Cost, transaction details and bank's certificate.
Customer
2. Transaction details and encrypted credit card info using bank's public key.
Merchant
4. Confirmation signed by bank's public key. Optional receipt for customer. (Digital signature)
3. Details from 2 passed along with merchant's version of transaction. (Digital signature)
Bank

Figure 20: 2KP Protocol

The final level, 3KP, requires public key certificates to be issued to all customers (Appendix A). All three parties use digital certificates adding more security to the transaction. The customer is required to sign the encrypted transaction details providing both the merchant and the bank proof that the customer made the purchase (Wayner, 1996).

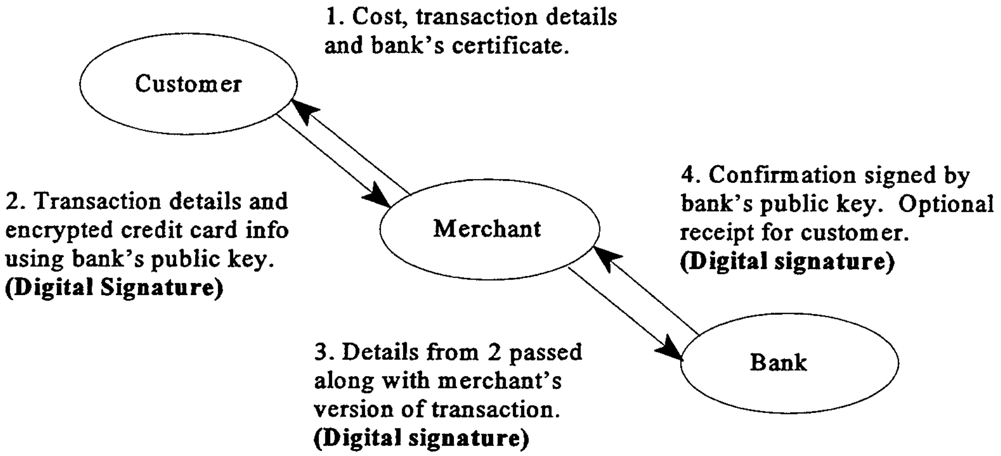

1. Cost, transaction details and bank's certificate.
Customer
2. Transaction details and encrypted credit card info using bank's public key. (Digital Signature)
Merchant
4. Confirmation signed by bank's public key. Optional receipt for customer. (Digital signature)
3. Details from 2 passed along with merchant's version of transaction. (Digital signature)
Bank

Figure 21: 3KP Protocol

Protocol Options

The iKP protocol provides for transaction options which are available to multiple sellers for the purpose of browsing and comparative shopping. The following transaction options are (Tsudik, 1996):

(1) SIG_B - Buyer's signature in the "PAYMENT" and "AUTH-REQUEST" mode. This option is at the discretion of the buyer the seller can refuse to issue an "INVOICE" if it is the seller's policy to always require an signature and the buyer is not able to provide it.

(2) SIG_S - Seller's signature in the "INVOICE" mode. This option is set by the buyer. However, the seller can refuse to comply if the buyer is not ready to pay.

(3) CONFIRM - Indicates that a "CONFIRM" is requested. This option is set by the buyer.

(4) SIG_A - Set by the buyer, this is option is used in conjunction with the "CONFIRM" option.

(5) CLRN - Authorization and clearance are performed together. This is set by the seller.

iKP Encryption

Use of encryption in the iKP protocol is limited to protecting the buyer's personal identification number (PIN) and buyer account number. RSA public key encryption is used to accomplish this (Appendix A).

Refunds

The buyer and seller need to run iKP using a negative amount, effectively crediting rather than debiting money to the buyer's account. The seller and the bank may require that the "CONFIRM" message from a purchase be associated with any refund. This will ensure that the transaction was valid and permits the seller to verify the original purchase transaction total (Tsudik, 1996).

Security Considerations

Public-key signature mechanisms are critically dependent upon the security of the corresponding private keys. iKP requires private and public keys of banks and optionally of sellers and buyers. iKP requires that public keys are distributed via certificates signed by well known certification authorities (Appendix A).

Conclusion

iKP is the electronic equivalent of the paper charge slip, signature and submission process. iKP takes input from the negotiation process (payment amount, order description, payment method) and causes the payment to happen via a three-way communication among the buyer, seller and the bank. The data required by iKP in the buyer's system are the bank's public key, the seller's public key, the buyer's account number, the buyer's public/private key pair, the buyer's personnel identification number (PIN), payment amount and currency, and the decryption of the order. The data required by iKP in the seller system are the bank's public key, seller's identification, seller's identification, seller's public/private key, payment amount and currency, and the description of the order. The IBM iKP protocols is an attempt to standardize the mechanism and the semantics for secure multi-party payments throughout the world on the World Wide Web.

E. SECURE ELECTRONIC TRANSACTION (SET) PROTOCOL

Introduction

Visa and MasterCard reported on February 1, 1996 (Visa and MasterCard press release, 1996) that they have been cooperating on a standard for the use of encryption technology for electronic payments on the Internet known as Secure Electronic Transaction (SET). Visa was allied with Microsoft Corp. and MasterCard with International Business Machines Corp. and Netscape Communications. Now they have come together to create SET as a standard on the World Wide Web for secure financial transactions (Evans, 1996).

Public key technology and symmetric algorithms are combined to ensure authentic and private electronic payments. Cryptographic algorithms and digital signatures using RSA technology are the tools which make the SET protocol secure and authentic. The SET protocol uses these tools to (SET draft, 1996):

(1) Provide confidentiality of information

(2) Ensure payment integrity

(3) Authenticate both merchants and cardholders

SET Technological Tools

The tools to a safe electronic shopping experience as specified by SET are digital certificates, public key encryption and digital signatures.

Digital Certificates

Digital certificates represent the heart of secure electronic transactions. Digital certificates provide an easy and convenient way to ensure that the participants in an electronic commerce transaction can trust each other. This trust is established through a common third party (Visa or MasterCard). Each party's SET compliant software validates both merchant and cardholder before any information is exchanged. The validation takes place by checking the digital certificates which were both issued by an authorized trusted third party (SET draft, 1996). Digital certificates ensure that all computers talking to each other can successfully conduct electronic commerce. The basis for this technology is public key encryption.

Public Key Encryption

Please see appendix A for public key encryption description.

Digital Signature

Digital signatures provides a method to associate the message with the sender. This authenticates the electronic purchase/payment transaction. SET uses these cryptographic techniques to provide information confidentiality, ensure payment integrity and authenticate both merchants and cardholders. Digital information security comprises all of these technologies to prevent the unauthorized disclosure, alteration or removal of information while controlling access of information moving across networks (SET draft, 1996).

SET Methodology

Cardholders must register their credit card directly on-line with their bank prior to any electronic purchases. The SET software provides a registration form on your PC screen with basic information (name, card account number, card expiration date, billing address). Once transmitted, this information is encrypted and securely sent to the computers of your credit card issuing financial institution. The bank will check to ensure the credit card account is authentic. The bank then issues an electronic certificate putting its digital signature on your digital certificate. The certificate is stored on your PC for future use. Similarly, merchants have to register to participate in secure shopping. The merchant's bank issues them a digital certificate allowing them to conduct electronic commerce.

The SET protocol uses three basic steps to protect credit card transactions from unauthorized use (SET draft, 1996).

(1) Before a customer sends a credit card number over the Internet, the personal computer scrambles it using Data Encryption Standard technology (Appendix A). The scrambled number is intended to be unintelligible to other Internet users even the merchant making the electronic sale.

(2) A special code lets the merchant check with the bank that issued the credit card, to confirm the validity of the number and the name of the credit card user.

(3) When the merchant gets the authorization from the bank, the sale goes through

without the merchant ever knowing the credit card number.

Conclusion

Visa and MasterCard jointly developed the Secure Electronic Transactions (SET) protocol as a method to secure bankcard transactions over the Internet. SET uses public key cryptography for confidentiality, payment integrity, authentication and nonrepudiation which are critical to both the customer and the merchant. SET is the standard for Visa and MasterCard to bring consumers and merchants together for secure electronic commerce.

F. SECURE HYPERTEXT TRANSFER PROTOCOL (S-HTTP)

Introduction

S-HTTP (Secure Hypertext Transfer Protocol) is a simple extension to the normal HTTP that was first proposed in Internet Draft in June of 1994 by Rescorla and Schiffman. The latest version (1.1) emerged in December of 1994 (Wayner, 1996). S-HTTP provides independently applicable security services for transaction confidentiality, authenticity/integrity and non-repudiability of origin (Rescorla, 1995). Current HTTP applications do not have the necessary support for cryptographic mechanisms appropriate for conducting commercial transactions.

S-HTTP provides secure communications between HTTP client/server allowing such transactions to be used for a wide range of applications. S-HTTP supports a variety of security mechanisms providing symmetric capabilities to both client and server while preserving the transaction model and implementation characteristics of the current HTTP (Rescorla, 1995). Cryptographic message formats such as PKCS-7, PEM and PGP support interoperation. S-HTTP supports "end-to-end" secure transactions in contrast with the existing HTTP mechanisms. Therefore, sensitive data do not need to be sent over the network in the clear (Rescorla, 1995).

Modes of Operation

The S-HTTP standard allows the traffic to and from the server to be either signed, encrypted, or authenticated in any combination (Wayner, 1996):

(1) Signature - If the digital signature enhancement is applied, an appropriate certificate may either be attached to the message or the sender may expect the recipient to obtain the required certificate independently.

(2) Encryption - Bulk encryption is supported by S-HTTP defines two key transfer mechanisms. The first method is public key (Appendix A) and another with externally arranged keys. In the former case, the symmetric key cryptosystem parameter is passed encrypted under the receiver's public key. In the latter mode, the content is encrypted using a prearranged session key, with key identification information specified on one of the header lines.

(3) Authentication - S-HTTP provides a means to verify sender authenticity and message integrity. Authentication is accomplished by using a hash function which provides a message digest (Appendix A). The message digest is then encrypted with a key and sent. This mechanism is useful in cases where it is appropriate to allow parties to identify each other reliably in a transaction without providing third-party non-repudiability for the transactions themselves. This mechanism is motivated by the idea that the action of "signing" a transaction should be explicit and conscious for the user, whereas many

authentication needs (access control) can be met with a lighter-weight mechanism that retains the scalability advantages of public-key cryptography (Rescorla, 1995).

HTTP Encapsulation

A secure HTTP message consists of a request or status line followed by a series of style headers and encapsulated content. When the content is decoded, it will be either another secure HTTP message, an HTTP message, or simple data. The request or status line, when accepted, will be considered non-coding and clients will substitute the URL of the request when communicating. Secure style header lines will be treated as case insensitive unless otherwise specified (Rescorla, 1995). The terminal encapsulated content message is largely dependent upon the values of the content privacy domain and content transfer encoding fields. Once the privacy enhancements have been removed, the contents will be a normal HTTP request. Alternatively, the content may be another secure HTTP request, which privacy enhancements will be unwrapped until clear content is obtained (Rescorla, 1995).

Message Format Options

PKCS-7

PKCS-7 (Cryptographic Message Syntax Standard) is a cryptographic message encapsulation format, similar to PEM, which was defined by RSA Laboratories as part of a family of related standards. The PKCS standards are offered by RSA to developers of computer systems employing public key cryptography. PKCS-7 is one of three encapsulation formats supported by S-HTTP, but it is preferred because it permits the least restricted set of negotiable options, and permits binary encoding. PKCS-7 is a superset of PEM, in that PEM messages can be converted to PKCS-7 messages without any cryptographic operations, and vice-versa and their key management materials (certificates) are also compatible (Rescorla, 1995).

Messages may be either signed, encrypted, both or neither. Appropriate certificates must be attached to digital signature messages. A certificate signed with the private component corresponding to the public component is referred to as a self-signed certificate. A purely signed message is precisely PKCS-7 compliant (Rescorla, 1995). Encryption using either a public key or a prearranged key is accomplished using PKCS-7. A message using PKCS-7 encryption may or may not be signed. While generating signed, encrypted data, it is necessary to generate the signed data production prior to encryption (Rescorla, 1995).

PEM/PGP

PEM (Privacy-Enhanced Electronic Mail) and PGP (Pretty Good Privacy) both use RSA encryption. RSA encryption provides integrity, data origin authenticity, and optionally, confidentiality (Kent, 1996). The only problem that PEM/PGP has had is that the messages are not time stamped. This means that a malicious user could record your encrypted message with a packet sniffer and repeat it back to the server. Even though the reply would be unreadable, if the request was something for which you were being charged, a large bill may be waiting for you at the end of the month (Rescorla, 1995).

Negotiation and Negotiation Headers

All parties communicating need to be able to negotiate which cryptographic method to use. The appropriate option choices will depend on implementation capabilities and the requirements of particular applications. A negotiation block is a sequence of specifications each conforming to a four-part schema detailing (Rescorla, 1995):

(1) Property - The option being negotiated (ie. bulk encryption algorithm).

(2) Value - The value being discussed for the property (ie. DES-CBC).

(3) Direction - The direction which is to be affected (ie. during reception or origination).

(4) Strength - Strength of preference (ie. required, optional, refused).

An example of a negotiation header (Rescorla, 1995):

STTP-Symmetric-Content-Algorithms: recv-optional=DES-CBC, RC4

S-HTTP-Privacy-Domains

New header lines are defined as necessary to permit negotiation of the application choices. All negotiation headers can be considered to apply to all privacy domains (message formats) or to a particular one. When specifying negotiation parameters which apply to all domains, the header lines need to be provided before any privacy-domain specifier. Negotiation headers which follow a privacy-domain header are considered to apply only to that domain. Multiple privacy-domain headers specifying the same privacy domain are permitted, in order to support multiple parameter combinations (Rescorla, 1995).

Security Retries for S-HTTP Requests

A request that is unsatisfactory for the reason of incorrect cryptographic enhancements may be repeated with the options found in the negotiation header. This method can be used to force a new public key negotiation if the session key in use has expired. The server may also require the client to retry the request using another set of cryptographic options. The client will perform the retry in the manner indicated by the combination of the original request, the precise nature of the error, and the cryptographic enhancements depending on the options the server requires (Rescorla, 1995). Automatic retries are rarely used due to potential compromise of encrypted information.

Transaction Security Status

A visual indication of the security of the transaction, and an indication of the party who will be able to read the message appear on the browser during secure message preparation. The browser will indicate the identity of the signer. Any failure to authenticate or decrypt an S-HTTP message will be presented differently from a failure to retrieve the document. This gives the client the option to display unverifiable documents (Rescorla, 1995).

Conclusion

Secure HTTP supports many security mechanisms providing security options for World Wide Web financial transactions. Traffic may either be signed, encrypted, or authenticated allowing nine different options in any combination (three for the client and three for the server). PKCS-7, PEM and PGP are cryptographic message format standards used to support S-HTTP clients and servers. S-HTTP message integrity verification is message based. When a message is correctly received, all packets in the stream are received. Secure HTTP interacts with HTTP messages in many ways. The negotiation structure offers the flexibility allowing the S-HTTP protocol to be used for a number of encryption solutions. Message integrity is computed on the entire message. Performance boosting schemes based on packetizing messages and multiplexing them over a single message stream is no longer required. No sensitive data will ever need to be sent over the World Wide Web in the clear with S-HTTP available.

G. SECURE SOCKETS LAYER V3.0 - SSL

Introduction

Secure Sockets Layer (SSL V3.0) is an open nonproprietary security protocol that provides communications privacy between application protocols over the Internet. This security protocol also provides data encryption, server authentication, message integrity, and optional client authentication for a TCP/IP connection. The protocol is composed of two layers. The layer below a reliable transport protocol is the SSL Record Protocol. The SSL Record Protocol encapsulates higher level protocols. One such protocol is the SSL Handshake protocol which allows the client and server to authenticate each other and to negotiate an encryption algorithm and cryptographic keys before the application protocol transmits or receives its first byte of data (Freier, 1996). The SSL protocol has three basic properties:

(1) The connection is private. Encryption is used after an initial handshake to define a secret key. Symmetric cryptography is used for data encryption. Examples are DES or RC4 (Appendix A).

(2) Identity can be authenticated using asymmetric, or public key, cryptography. Examples are RSA or DSS (Appendix A).

(3) The connection is reliable. Secure hash functions such as SHA or MD5 (Appendix A) are utilized (Freier, 1996).

There is broad support for this protocol which will support interoperability between products from many organizations. Apple Computer, Inc., Bank of America, ConnectSoft, Delphi Internet Services Corporation, Digital Equipment Corporation, First Data Corporation, IBM, MarketNet, MasterCard International Inc,. MCI Communications Corp., Microsoft Corporation, Novel Inc., Open Market, Prodigy, Silicon Graphics, Inc., StarNine, Sun Microsystems, Inc., Visa International, and Wells Fargo are among companies backing SSL (Netscape press release, 1996).

SSL Protocol Technical Attributes

SSL provides a security handshake during initiation of a TCP/IP connection. The handshake results in an agreement between client and server on the level of security that will be used. SSL requires servers to maintain certificates which are issued by a Certificate Authority (CA). Certificates verify the legitimacy of arbitrary servers (Appendix A). Thereafter, SSL is only providing encryption and decryption (DES or RC4) of the application protocol being used (Freier, 1996).

SSL messages can include fields for length, description, and content. Since SSL is a layered protocol, the message fields are included at each layer. When the message is ready for transmission, SSL fragments the data into blocks, compresses the data if necessary, encrypts and transmits. Data received are then decrypted, verified, decompressed and reassembled before being delivered to higher level clients (Freier, 1996).

Session and Connection States

The SSL session is stateful, which means that the protocol controls and coordinates the read and write states of both client and server. The protocol state machines are then allowed to operate consistently, despite the fact that the state is not exactly parallel (Freier, 1996). The state is repeated twice, once during the current state and again during the handshake protocol. Additionally, separated read and write states are maintained. When the client or server receives a change cipher spec message, it copies the pending read state into the current read state. When the client or server sends a change cipher spec message, it copies the pending write state into the current write state (Freier, 1996). When the handshake negotiation is complete, the client and server exchange change cipher spec messages and they then communicate using the newly agreed upon cipher spec. An SSL session may include multiple secure connections; in addition, parties may have multiple simultaneous sessions (Freier, 1996).

The session state includes the following elements (Freier, 1996):

(1) Session Identifier - An arbitrary byte sequence chosen by the server to identify an active or resumable session state.

(2) Peer Certificate - Certificate of the peer. This element of the state may be null.

(3) Compression Method - The algorithm used to compress data prior to encryption.

(4) Cipher Spec - Specifies the bulk data encryption algorithm such as null or DES (Appendix A) and a message authentication code (hash) algorithm such as MD5 or SHA (Appendix A). It also defines cryptographic attributes such as the hash size.

(5) Master Secret - 48 byte secret shared between the client and server.

(6) Resumable - A flag indicating whether the session can be used to initiate new connections.

The connection state includes the following elements (Freier, 1996):

(1) Server and Client Random - Byte sequences that are chosen by the server and client for each connection.

(2) Server Write Hash Secret - The secret used in hash operations on data written by the server.

(3) Client Write Hash Secret - The secret used in hash operations on data written by the client.

(4) Server Write Key - The symmetric bulk cipher key for data encrypted by the server and decrypted by the client.

(5) Client Write Key - The symmetric bulk cipher key for data encrypted by the client and decrypted by the server.

(6) Initialization Vectors - When a symmetric block cipher in CBC mode (Appendix A) is used, an initialization vector (IV) is maintained for each key. This field is first initialized by the SSL handshake protocol. Thereafter the final ciphertext block from each record is preserved for use with the following record.

(7) Sequence Numbers - Each party maintains separate sequence numbers for transmitted and received messages for each connection. When a party sends or receives a change cipher spec message, the appropriate sequence number is set to zero.

Record Layer

The SSL Record Layer receives uninterpreted data from higher layers in non-empty blocks of arbitrary size. The record layer fragments information blocks into SSLPlaintext records of 2^14 bytes or less (Freier, 1996). Client message boundaries are not preserved in the record layer. Multiple client messages of the same Content type may be coalesced into a single SSLPlaintext record. Data of different SSL Record layer content types may be used together. Application data is generally of lower precedence for transmission than other content types.

Record Compression and Decompression

All records are compressed using the compression algorithm defined in the current session state. There is always an active compression algorithm. However, initially it is defined as CompressionMethod.null (Freier, 1996). The SSLPlaintext is compressed into an SSLCompressed structure. Compression erases state information as the CipherSpec is replaced. Compression must be lossless and may not increase the content length by more than 1024 bytes (Freier, 1996). If the decompression function encounters an SSLCompressed.fragment that would decompress to a length in excess of 2^14 bytes, it will issue an error alert.

Handshake Protocol

The SSL Handshake Protocol is one of the defined higher level clients of the SSL Record Protocol. This protocol is used to negotiate the secure attributes of a session. Handshake messages are supplied to the SSL Record Layer, where they are encapsulated within one or more SSLPlaintext structures, which are processed and transmitted as specified by the current active session state (Freier, 1996). The cryptographic parameters of the session state are produced by the SSL Handshake Protocol on top of the SSL Record Layer. When a SSL client and server first begin communicating, they agree on a protocol version, select cryptographic algorithms, optionally authenticate each other, and use public-key encryption (Appendix A) techniques to generate symmetric session keys.

The client sends a client hello message to which the server must respond with a server hello message, or else a fatal error will occur and the connection will fail. The client hello and server hello are used to establish security enhancement capabilities between client and server. The client hello and server hello establish the following attributes: Protocol Version, Session ID, Cipher Suite, and Compression Method (Freier, 1996).

Following the hello messages, the server will send its certificate, if it is to be authenticated (Netscape, 1996). Additionally, a server key exchange message may be sent, if it is required. If the server is authenticated, it may request a certificate from the client. Now the server will send the server hello done message, indicating that the hello-message phase of the handshake is complete (Freier, 1996). The server will then wait for a client response. If the server has sent a certificate request message, the client must send either the certificate message or a no certificate alert. The client key exchange message is now sent. The content of that message will depend on the public key algorithm selected between the client hello and the server hello. If the client has sent a certificate with signing ability, a digitally-signed certificate verify message is sent to verify the certificate (Netscape, 1996).

When a change cipher spec message is sent by the client, the client copies the pending Cipher Spec into the current Cipher Spec. The client then immediately sends the finished messages using the new algorithms. In response, the server will send its own change cipher spec message, transfer the pending to the current Cipher Spec (Freier, 1996). The handshake is complete and the client and server may begin to exchange application layer data.

When the client and server decide to resume a previous session or duplicate an existing session Freier defines the message flow as follows: The client sends a ClientHello using the Session ID of the session to be resumed. The server then checks its session cache for a match. If a match is found, and the server is willing to re-establish the connection under the specified session state, it will send a ServerHello with the same Session ID value. Both client and server must send change cipher spec messages and proceed directly to finished messages. Once the re-establishment is complete, the client and server may begin to exchange application layer data. If a Session ID match is not found, the server generates a new Session ID and the SSL client and server perform a full handshake.

Record Payload Protection and the CipherSpec

All records are protected using the encryption and hash algorithms defined in the current CipherSpec. There is always an active CipherSpec. However, initially it is set to null, which does not provide any security (Freier, 1996).

When the handshake is completed, the two parties communicating have shared the necessary secrets which are used to encrypt records and compute hash functions. The hash operations and techniques used to perform the encryption are defined by the CipherSpec (Freier, 1996). The encryption, decryption and hash functions translate the SSLCompressed structure into SSLCiphertext and sequencing numbers. The sequencing numbers allow detection of missing or altered messages (Freier, 1996).

Asymmetric Stream Cipher

Stream ciphers (Appendix A) convert SSLCompressed fragment structures to and from stream SSLCiphertext fragment structures (Freier, 1996). The hash is computed before encryption. The stream cipher encrypts the entire block, including the hash. Stream ciphers that do not use a synchronization vector such as RC4 (Appendix A), simply use the stream cipher state from the end of one record on the subsequent packet (Freier, 1996).

CBC Block Cipher

The encryption and hash functions convert SSLCompressed fragment structures to and from block SSLCiphertext fragment structures when using symmetric block ciphers (Appendix A). The initialization vector (IV) for the first record is provided by the handshake protocol when using CBC. The IV for subsequent records is the last ciphertext block from the previous record (Freier, 1996).

Change Cipher Spec Protocol

The change cipher spec protocol exists to signal transitions in ciphering strategies. The protocol consists of a single message, which is encrypted and compressed under the current CipherSpec. The change cipher spec message is sent by both the client and server to notify the receiving party that subsequent records will be protected under the newly negotiated CipherSpec and keys. Reception of this message causes the receiver to copy the read pending state into the read current state. The client sends a change cipher spec message following handshake key exchange and certificate verify messages and the server sends one after successfully processing the key exchange message it received from the client. An unexpected change cipher spec message should generate an unexpected message error alert (Freier, 1996).

Finished

A finished message is always sent immediately after a change cipher specs message to verify that the key exchange and authentication processes were successful. The finished message is the first protected with the newly negotiated algorithms. No acknowledgment of the finished message is required. Parties may begin sending confidential data immediately after sending the finished message. Recipients of finished messages must verify that the contents are correct. The hash contained in finished messages sent by the server incorporate Sender.server; those sent by the client incorporate Sender.client (Freier, 1996). The value handshake messages includes all handshake messages starting at client hello up to, but not including the finished messages (Freier, 1996).

Alert Protocol

One of the content types supported by the SSL Record layer is the alert type. Alert messages convey the severity of the message and a description of the alert. Immediate termination may occur. However, other connections corresponding to the session may continue, but the session identifier must be invalidated, preventing the failed session from being used to establish new connections. Like other messages, alert messages are encrypted and compressed, as specified by the current connection state (Freier, 1996).

Closure Alerts

The client and the server must share knowledge that the connection is ending in order to avoid truncation. Either party may initiate the exchange of closing messages. A close notification is an example of a closure alert. This message notifies the recipient that the sender will not end any more messages on this connection. The session becomes unresumable if any connection is terminated without proper notification messages with a level equal to the warning (Freier, 1996).

Error Alerts

Error handling in the SSL handshake protocol is fairly simple. As an error is detected, a message is sent to the other party. Upon transmission or receipt of a fatal alert message, both parties close the connection immediately. Clients and servers are required to delete any session identifiers, keys and secrets associated with the failed connection (Freier, 1996).

Security Analysis

The SSL protocol is designed to establish a secure connection between a client and a server communicating over an insecure channel. Assuming that attackers have substantial computational resources, they may have the ability to capture, modify, delete, replay, and tamper with messages sent over any communication channel (Netscape, 1996). The handshake protocol is responsible for selecting a CipherSpec and generating a MasterSecret, which together comprise the primary cryptographic parameters associated with a secure session. The handshake protocol can also optionally authenticate parties who have certificates signed by a trusted certificate authority (Freier, 1996).

RSA Key Exchange and Authentication

RSA, Key exchange and server authentication are combined using RSA cryptography. The public key may be either contained in the server's certificate or may be a RSA session key (Appendix A). When RSA session keys are used, they are signed by the server's RSA or DSS certificate. Servers may use a single RSA session key for multiple negotiation sessions. The server's certificate is the first verified, then the client encrypts a pre master secret with the server's public key (Freier, 1996). Successfully decoding the pre master secret and producing a correct finished message allows the server to demonstrate that it knows the private key corresponding to the server certificate (Freier, 1996). The client signs a value derived from the master secret and all preceding handshake messages. These handshake messages include the server certificate, which binds the signature to the server, and ServerHello.random, which binds the signature to the current handshake process (Freier, 1996).

Diffie-Hellman Key Exchange with Authentication

When Diffie-Hellman key exchange is used, the server can either supply a certificate containing fixed Diffie-Hellman parameters or can send a set of temporary Diffie-Hellman parameters signed with a DSS or RSA certificate. Temporary parameters are hashed with the hello.random values before signing to ensure that attackers do not replay old parameters (Freier, 1996). The client, in either case, can verify the certificate or signature to ensure that the parameters belong to the server.

If the client has a certificate containing fixed Diffie-Hellman parameters, its certificate contains the information required to complete the key exchange. To prevent the pre master secret from staying in memory any longer than necessary, it should be converted into the master secret as soon as possible (Freier, 1996). Client Diffie-Hellman parameters must be compatible with those supplied by the server for the key exchange to work (Freier, 1996).

Fortezza

Fortezza's design is classified, but at the protocol level it is similar to Diffie-Hellman with fixed public values contained in certificates. The result of the key exchange process is the token encryption key (TEK), which is used to wrap data encryption keys, client write key, server write key, and the master secret encryption key (Freier, 1996). The data encryption keys are not derived from the pre master secret because unwrapped keys are not accessible outside the token (Freier, 1996). The encrypted pre master secret is sent to the server in a client key exchange message (Freier, 1996).

Detecting Attacks Against the Handshake Protocol

An attacker might try to influence the handshake exchange to make the parties select different encryption algorithms than they would normally choose. Because many implementations will support 40-bit exportable encryption and some may even support null encryption or hash algorithms, this attack is of particular concern (Netscape, 1996). An attacker must actively change one or more handshake messages to invite this attack. If this occurs, the client and server will compute different hash values for the handshake messages. As a result, the parties will not accept each others' finished messages. Without the master secret, an attacker cannot repair the finished messages, so an attack will be discovered (Freier, 1996).

Conclusion

SSL can provide effective electronic communications security between parties providing the client and server systems, keys, and applications are secure and free from security errors. The system is only as strong as the weakest key exchange and authentication algorithm supported, and only trustworthy cryptographic functions should be used. Short public keys, 40-bit bulk encryption keys, and anonymous servers should not be used. Implementations and users must be careful when deciding which certificates and certificate authorities are acceptable.

VI. FINANCIAL TRANSACTION SERVICE COMPANIES

A. BROADVISION INC.

Introduction

BroadVision Inc. has developed a one-to-one application system for dynamic, personalized marketing and selling on the Internet. The one-to-one software product transforms static Web sites into interactive marketing communities by empowering business managers to create and deliver personalized services that save consumers time, effort, and money (Runge, 1996). Using the product's innovative Dynamic Command Center feature, marketing, advertising, and Web content manages can perform the following (Runge, 1996):

(1) Personalize editorial content, advertising and incentive programs based on individual consumer demographics and usage patterns.

(2) Observe consumer interactions in real time to identify and seize opportunities based on consumers' on-line activity.

(3) Foster virtual communities by integrating electronic mail bulletin boards and on-line forums.

(4) Establish collaborative on-line dialogues with customers to improve long-term satisfaction and retention. BroadVision Inc. was founded in May 1993 by Dr. Pehong Chen (Runge, 1996).

Application System Architecture

The application system offers a scalable three-tiered architecture permitting business rules to be created and modified independent of application logic and data sources (Runge, 1996). This enables business managers to react fast to changing business conditions without compromising integrity of data and application logic.

Security and External Business Systems

BroadVision uses RSA cryptography to safeguard credit card numbers and transaction information. BroadVision one-to-one application can also be used with the Secure Sockets Layer (SSL) protocol (BroadVision, 1996). BroadVision's open standards-based Common Object Request Broker Architecture (CORBA) interfaces allow one-to-one applications to interoperate with any external business system (BroadVision, 1996).

CyberCash and VeriFone Payment Support

One-to-one supports CyberCash and VeriFone technologies for electronic payment of transactions conducted over the Internet. The CyberCash Secure Internet Payment System provides safe, convenient and immediate processing of transactions and authorization codes between consumers, merchants and their banks in real-time (BroadVision, 1996). VeriFone's Internet Transaction Switch provides a range of payment functions, including transaction switching and credit/debit authorization settlement support (BroadVision, 1996).

Electronic Data Interchange (EDI)

EDI provides an inexpensive, and secure forwarding of purchase orders, invoices, shipping notices, and other frequently used business documents between applications and computers (BroadVision, 1996).

Personalized Home Pages

The one-to-one Web Content Development Tool is used to build page templates and content management can be defined and maintained in the Dynamic Command Center (BroadVision, 1996). Building page templates is similar to creating a traditional static Web page. One-to-one generates content dynamically based on business rules and personal aspects of the dialogue with the consumer. A unique Web page can be generated for each individual every time a page template is accessed.

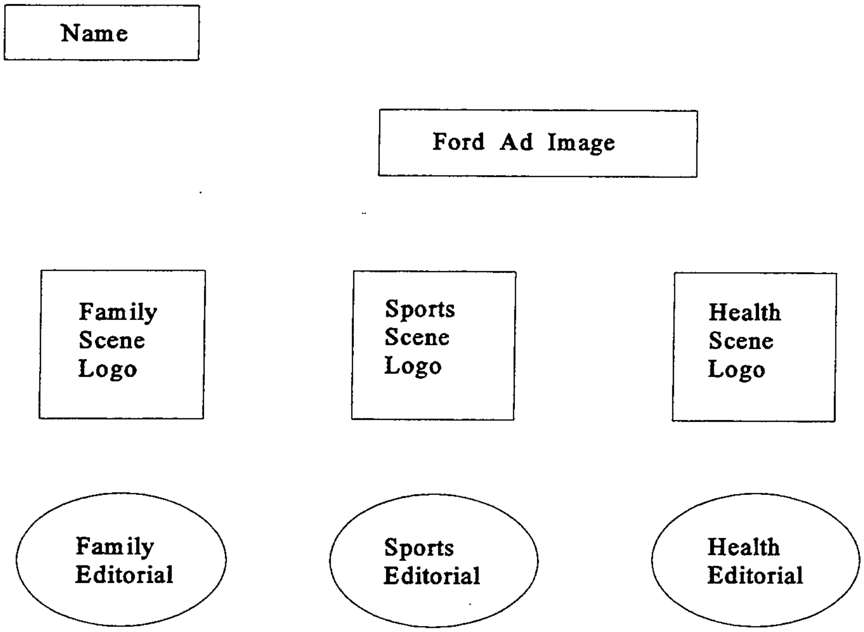


Figure 22: Example Personalized Home Page

Methodology

BroadVision has developed a model for creating successful one-to-one on-line marketing and selling systems (BroadVision, 1996).

(1) Attract and retain consumers by providing personalized and compelling content

couple with a sense of community relevant to them.

(2) Engage consumers in personalized dialogue, learning more about their needs to better anticipate their future needs and requirements.

(3) Motivate consumers by providing personalized incentives (i.e. coupons and ads) for them to move from dialogue to action such as ordering a product or completing a survey.

(4) Fulfill transactions by reliably and securely supporting the full spectrum of electronic commerce from promotional pricing to secure payment handling.

(5) Manage the process by monitoring results and allowing dynamic changes to business rules and content to ensure the system is achieving business goals.

Conclusion

The principal users of BroadVision one-to-one application are business people who research, design, redesign and run all business functions of a Web site (BroadVision, 1996). Traditionally, business people have had to rely on computer programmers to implement marketing programs, selling models, and business rules using fairly complicated programming (Runge, 1996). BroadVision's one-to-one application allows businesses to respond quickly to changes in the marketplace by easily changing Web site content and personalizing it for individual consumers.

B. CONNECT INC. ONESERVER ORDERSTREAM

Introduction

Connect Inc., founded in 1987, is based in Mountain View, California. Connect is a provider of Internet-based interactive commerce and order management applications for companies that want to use the Internet for electronic commerce (Strohecker, 1996). The company also provides high-end software and services adding a decade of on-line experience (Strohecker, 1996). RSA Data Security, Inc. has teamed up with Connect Inc. and provides technology backing for Connect's electronic commerce secure OneServer OrderStream platform.

OneServer Features

OneServer can transparently access data in either the OneServer database or within external database systems. OneServer is the only Internet commerce server with three levels of security (Strohecker, 1996).

(1) OneServer applications platform compliments RSA encryption with internal access protection.

(2) Connect provides technology controls to prohibit unauthorized access.

(3) Connect's technology also limits authorized users to specific transactions.

OneServer software is based on industry standard database and operating system technology providing businesses with functionality, maximum flexibility, scalability and manageability for electronic commerce applications (Strohecker, 1996). OneServer features include integrated dynamic data query and simplified page layout functions which allow businesses to provide access to large volumes of graphics and data (Strohecker, 1996). Therefore, products are more easily tracked and sold on-line and businesses can customize consumer interfaces.

JICA (Java Interactive Commerce Applet)

The combination of Sun's Java programming language and Connect's OneServer software allows businesses to build experience of a trained salesperson, including the salesperson's knowledge base of various products into an on-line Interactive Commerce application (Connect Press Release, 1996). Businesses can allow customers to access this electronic salesperson for an informative description of products on-line and apply it to purchases.

Logica Multimedia Solution

Logica Inc., founded in 1969, provides software and services to the finance, telecommunications, computing and electronic companies in more than 18 countries (Connect Press Release, 1996). Logica is in the process of developing large-scale interactive commerce applications based on the Connect OneServer software platform. Logica and Connect hope that this alliance will extend the reach of electronic commerce and provide a multimedia application allowing effective marketing of products and services worldwide.

VeriSign Digital Certificates

VeriSign augments OneServer security by electronically authenticating and issuing digital certificates for conducting business to business electronic financial transactions. Digital identification technology provides a trusted method of authenticating the identity of parties during electronic financial transactions (Connect Press Release, 1996). Digital certificates are issued by a trusted third party (i.e. VeriSign) that performs background checks on individuals or businesses. Public key cryptography techniques are used to bind the owner's unique digital key into a file that is digitally signed by the issuing agent (Appendix A). VeriSign signs its digital identifications with the longest encryption key sizes currently deployable in commercial applications (Strohecker, 1996).

OneServer OrderStream

OrderStream is a complete, secure Internet application that streamlines and automates the sales channel for business to business distributors. OrderStream is built on the OneServer software platform and supports distribution of computers, software, electronics parts, office equipment and supplies (Connect Press Release, 1996). OrderStream allows distributors to take volume orders quickly and easily over the Internet enabling companies to maximize profits at lower costs.

Conclusion

OrderStream built on OneServer software architecture was introduced in September 1995. OneServer is based on UNIX and the Internet. The platform supports all Web browsers and provides enhanced features for corporate developers who are customizing solutions for interactive commerce.

C. CYBERCASH INC.

Introduction

CyberCash Inc. of Reston, Virginia, founded in August 1994 is a developer of software service solutions for secure electronic financial transactions over the Internet. The CyberCash system is designed to allow banks to offer secure Internet payments and micropayments to merchants. CyberCash works with all credit card processing institutions, enabling payments by credit card to be instantaneously processed (Claymon, 1996). Electronic check and electronic coin services are expected to be released in late 1996 (CyberCash Press Release, 1996). CyberCash system includes consumer software, merchant software, and gateway services.

CyberCash Functionality

The foundations of the CyberCash system are encryption and digital signatures provided by RSA Data Security software (Wayner, 1996). The software operates on Microsoft Windows and will operate on Macintosh and UNIX platforms by late 1996 (CyberCash Press Release, 1996).

The basic credit card transactions are very similar in structure to the IBM iKP system. Customers set up accounts by downloading software from CyberCash and filling out an application form. The customers include the credit card numbers that they plan to use. CyberCash creates an individualized encrypted file for each customer that includes their credit card number and a public key that are assigned by CyberCash (Wayner, 1996). This preprocessing allows CyberCash the opportunity to ensure the credit card is valid with the issuing bank.

CyberCash Credit Card Transaction

The steps in CyberCash credit card transactions are (CyberCash, 1996):

(1) A consumer has shopped the merchant's site ad and decides to make a purchase and where to ship merchandise. The merchant server returns the price of the item.

(2) The consumer selects the "pay" button which sends the order and encrypted payment information to the merchant.

(3) The merchant receives the packet, strips off the order and forwards the encrypted payment information digitally signed and encrypted with his private key to the CyberCash server. The merchant cannot see the consumer's credit card information.

(4) The CyberCash server receives the packet, takes the transaction behind its firewall

and off the Internet, unwraps the data, reformats the transaction and forwards it to the merchant's bank over dedicated lines.

(5) The merchant's bank then forwards the authorization request to the issuing bank conventionally. The approval or denial code is sent back to CyberCash.

(6) CyberCash returns the approval or denial code to the merchant who passes it onto the consumer. Step one to step six takes 15 - 20 seconds.

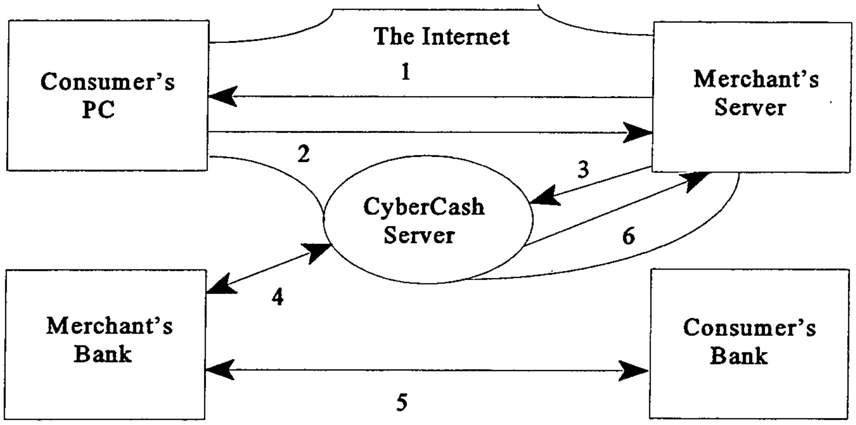


Figure 23: CyberCash Secure Internet Credit Card Payment Transaction

Conclusion

CyberCash client software package is exportable and designed to negotiate firewalls. CyberCash has agreements with several merchants (Digital Equipment Corp., Sun Microsystems, First of Omaha Merchant Processing, CheckFree, National Data Corp., and Xerox) and two major banks (Bank of America and Wells Fargo). The major difference between the CyberCash system and IBM iKP protocol is the need for certificates. CyberCash issues the public key pairs for all users and maintains certificate authority.

D. FIRST VIRTUAL HOLDINGS INC.

Introduction

First Virtual Holdings Inc. introduced the world's first fully operational Internet payment and micropayment system in October 1994 (Gable, 1996). The company was created specifically to enable safe global buying and selling by anyone with access to the Internet. The system is electronic mail (e-mail) based that transfers money by passing e-mail messages. The system is operated by a green commerce server located in Austin, Texas (Chapter V). The transactions are simple and straight forward. Both buyer and seller must have First Virtual accounts which are associated with conventional methods of deposits and payments. Checking and bankcard account numbers are never typed on a keyboard or sent over the Internet.

The Concept

The payment system accomplishes safe transactions without the need for Internet users to purchase or install additional software or equipment (Borenstein, 1995). Existing e-mail technology is used without cryptography. E-mail call-backs provide security to all cardholders when their Virtual PIN is in use. Encryption is not used for the following reasons (Borenstein, 1995):

(1) Encryption and signature technologies prevent most people from participating.

(2) Encryption and signature technologies are complicated and confusing.

(3) Encryption and signature technologies yield a false sense of security.

(4) Encryption and signature technologies require the use of software and certification infrastructures that are not commonly available.

(5) Encryption and signature technologies are restricted by patents, copyrights, and export restrictions.

Becoming a Buyer

Complete an application on the Internet and receive a Virtual PIN. Part of this process requires registration with a credit card over the telephone (FV Information, 1996). A valid Visa or MasterCard and an Internet e-mail address are required. When making a purchase, provide the merchant the Virtual PIN. First Virtual's green commerce server will send an e-mail confirming the purchase and wait for the buyer's response (Chapter V).

Becoming a Merchant

Complete an application on the Internet and receive a Virtual PIN. A bank account that accepts direct deposit is required with a ten-dollar registration fee (FV Information, 1996). Send an e-mail message containing the buyer's Virtual PIN and the amount of sale. The green commerce server confirms the transaction with the buyer and notifies the merchant via e-mail (Chapter V).

<u>Virtual PIN Security</u>

The green commerce server settles all buying-selling transactions off-line (Chapter V). Transactions are confirmed with buyers via e-mail before any charges are applied to a credit card. Credit card numbers are never typed on a keyboard. The Virtual PIN is the only number typed and sent over the Internet eliminating the need for encryption and significantly reducing the potential for fraud (Borenstein, 1996).

First Virtual Fees

The cost to register with FV is two dollars for consumers and ten dollars for sellers. Sellers pay a 29-cent fee and two percent of the transaction price for each transaction. Sellers are also charged one dollar processing fee each time a payment is made to their bank account. (FV Information, 1996)

Equity Partners

(1) First USA Merchant Services, Inc., Dallas, Texas.

(2) National Direct Marketing Corp. (NDMC), Arlington, Virginia.

(3) Sybase, Inc. (Sybase), Emeryville, California.

Strategic Alliances

(1) Electronic Data Systems (EDS)

(2) Network Computing Devices (NCD)

(3) Spyglass, Inc.

(4) Sun Microsystems Computer Corp. (SMCC)

The Founders

(1) Nathaniel S. Borenstein, Ph.D., chief scientist.

(2) Marshall T. Rose, Ph.D., principal developer.

(3) Einar A. Stefferud, MBA, founder.

(4) Lee H. Stein, J.D., chairman and CEO.

Conclusion

First Virtual is a simple, safe, and conservative approach to Internet commerce. No criminal has broken into the system and no flaws have been discovered in the first year of operation (Borenstein, 1996). Merchants are not attractive targets for criminals because they do not collect credit card numbers. Buyers do not have to obtain, install, and learn to use new software. No export or licensing restrictions are involved in the use of the system. However, credit card and bank account numbers are given over the telephone and e-mail messages can be intercepted and manipulated.

E. NETSCAPE COMMERCE SERVER

Introduction

Netscape Communications Corp. based in Mountain View, California was founded in April 1994 by Dr. James H. Clark, founder of Silicon Graphics, Inc. (Netscape Press Release, 1995). Netscape Communications have developed the Internet's first secure server, the Netscape Commerce Server, which incorporates the Secure Sockets Layer (SSL) protocol (Chapter V). When paired with Netscape Navigator or other Internet navigators supporting SSL, the Netscape Commerce Server lets users take advantage of such commercial services as on-line publications, financial services and interactive shopping. The Netscape Commerce Server is high performance server software for conducting secure electronic commerce and communications on the Internet and other TCP/IP based networks. The server enables business on the Internet to gather customer feedback, conduct market research, and build extensive customer databases quickly and efficiently (Netscape, 1996).

Integrated Security

Advanced security features are provided using the SSL protocol (Chapter V). These features are designed to enable secure electronic commerce and communications. Flexible user authorization controls access to individual files or directories using a username and password, domain name, host name, IP address, or named groups (Netscape, 1996). SSL provides (Chapter V):

(1) Server authentication allowing any SSL compatible client to verify the identity of the server using a certificate and a digital signature.

(2) Data encryption ensuring the privacy of client-server communications by encrypting the data stream between them.

(3) Data integrity which verifies that the contents of a message arrive at their destination in the same form as they were sent.

SSL employs public key cryptographic technology from RSA Data Security. The Netscape Commerce Server requires a signed digital certificate to operate securely (Netscape, 1996).

Netscape Commerce Server Overview

Netscape Commerce server allows hypermedia documents to be published using the HyperText Markup Language (HTML) and deliver them over the Internet and other TCP/IP networks using the HyperText Transport Protocol (HTTP) (Netscape, 1996). Improved process and memory management enable Netscape Commerce Server to deliver unparalleled performance and reliability. Documents are delivered several times faster with a throughput several times higher than other available HTTP servers. The efficient process management features of Netscape Commerce Server minimize system load and increase overall server reliability. (Netscape, 1996)

Server Management

Netscape Commerce Server uses Netscape Navigator's graphical interface to provide a consistent, easy-to-use operating environment. The simple user interface and forms capability provide point and click server installation, configuration, and maintenance. Netscape Navigator and its forms capability for server management ensure a common look across all Netscape server products and enables secure remote configuration and management from any computer on the network. Forms are used for the initial server configuration managing all server functions including user authorization, transaction logging, and process configuration. (Netscape, 1996)

Conclusion

Organizations can rely on the Netscape Commerce Server to manage secure electronic financial transactions and communications across the Internet. SSL provides strong security to existing applications on the Internet incorporating RSA Data Security technology. Netscape is only producing U.S. version of the Netscape Commerce Server with the 128-bit RC4 (Appendix A) due to the current U.S. export laws (Netscape, 1996). The Netscape Commerce Server provides easy configurability and maintenance, full documentation and technical support.

F. OPEN MARKET

Introduction

The Open Market (OM) Web-based secure financial transaction system was developed by Open Market Inc. of Cambridge, MA in October 1994 (Wayner, 1996). OM first introduced Merchant Solution, a secure World-Wide Web server kit for businesses that handles financial transaction, order taking and payments, credit card transactions, sales tax processing, and other purchasing and distribution tasks over the Internet (Bowen, 1995). The OM Secure Web Server is the only Web server on the market that supports both the SSL and the S-HTTP security protocols (Chapter V). The OM Secure Web Server does not need to create session keys, which come from the browser in the SSL mode (OM Press Release, 1996). The OM Secure Web Server creates session keys, in the S-HTTP mode (OM Press Release, 1996). The OM Secure Web Server is the world's fastest achieving 5,000 simultaneous 14.4 Kb modem connections (King, 1996).

OM-SecureLink Executive

The newest class of software that OM has produced to perform Secure Electronic Commerce is OM - SecureLink Executive (OM Press Release, 1996). This consists of OM - Transact which is a complete back-office transaction management infrastructure for secure Internet commerce and OM-Access which are server software that centrally manages access to corporate data distributed across the World Wide Web (Gifford, 1996). OM - SecureLink Executive provides the following (OM, 1996):

(1) Change existing Website content into an online store.

(2) Securely manage user access to distributed Web content across heterogeneous servers.

(3) Track anonymous sessions and capture valuable information that will help manage Website content.

OM - Transact

OM - Transact enables companies to offer secure payment, complete order management, and online customer service. OM - Transact will support Electronic Data Interchange (EDI), purchase orders, and comprehensive reporting, in addition to SSL and S-HTTP (OM, 1996). OM - Transact is available to corporate users for a base price of $250,000 (OM, 1996).

OM - Transact features are (OM, 1996):

(1) Security: Keyed message authentication codes are used to ensure message integrity and secure payment protocols (SSL and S-HTTP).

(2) Authentication: Provides access control for registered buyers.

(3) Order Management: Securely accept orders using standard Web technologies.

(4) Record Keeping: Online, real-time transaction records for merchants (audit trail).

(5) Transaction Processing: Secure transaction and payment processing, automatically calculating shipping charges.

(6) Customer Service: Online account statements and customer service providing order status.

(7) Flexible Payment Model: Companies may offer products and services that can be paid in installments, subscription, or through a one-time charge.

The steps in the OM - Transact Model are (OM, 1996):

(1) Buyer requests a commerce enabled page

(2) The merchant serves up content with digital offers which contain the signed offer of a good or service for sale.

(3) The buyer selects on a digital offer to purchase an item.

(4) Service provider authorizes the purchase and settles charges.

(5) Service provider issues a digital receipt.

(6) OM - SecureLink Executive validates the digital receipt and serves the requested content.

(7) Service provider advises merchant of buyer's order.

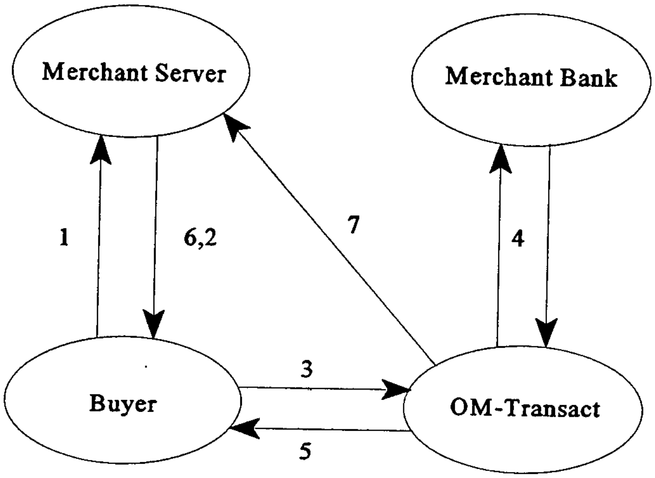


Figure 24: OM - Transact Model

OM - Transact allows merchants to sell goods and services directly from a Website. OM - SecureLink generates digital offers which contain unique keyed messages (hash). Prior to processing any orders, OM - Transact validates each hash. Merchants can be certain that goods and services are paid for when they are accessed from a Web site. Customers will receive a digital receipt that the OM - Transact generates validating their purchase. (OM, 1996)

OM - Access

OM - Access is the server software designed to support a company's Web applications by centrally managing the authentication and authorization of end users. OM - Access solves information management problems by identifying users, controlling access to data by individual and group, measuring and reporting access to data across multi-vendor servers, providing Web access to existing corporate systems, and enabling new Web-based applications (OM, 1996).

OM - Access features are (OM, 1996):

(1) OM - Access includes OM Secure Web Server software and analysis software.

(2) Flexible access to authorization databases through a published application programming interface (Chapter V).

(3) Ability to manage content stored on servers other than Open Market's.

(4) Secure control of access to information.

(5) Comprehensive auditing and reporting.

(6) Provides personalized content generation.

The steps in the OM - Access Model are (OM, 1996):

(1) Browser requests information.

(2) OM-SecureLink Executive denies access without a ticket.

(3) OM-Access authenticates and authorizes user, then grants ticket.

(4) OM-SecureLink Executive validates ticket and allows access.

(5) Requested information returned to validated user.

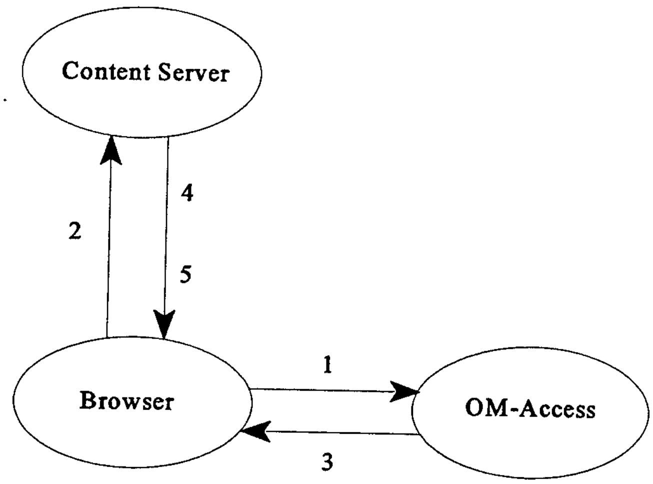


Figure 25: OM - Access Model

OM - Access can restrict access to your sensitive company information even if that information is stored on distributed content servers. Users must have tickets known as session identifiers in order to gain access to an associated company. Authentication is required prior to users receipt of authorized tickets and access. (OM, 1996)

Management

(1) Shikhar Ghosh, Chairman

(2) Gary Eichhorn, CEO

(3) David Gifford, cofounder and chief scientific officer

Conclusion

The Open Market system is easy to access and use. The system is an excellent way to set up a storefront and operate in an integrated electronic commerce environment. OM and FV are almost exact opposites. The fundamental difference is the level of trust

(Wayner, 1996). FV allows people to try before they buy and OM is designed for real-time transfer so payment is made before the information/goods are shipped. FV relies exclusively on electronic mail (e-mail) which can be slow. OM uses both SSL and S-HTTP protocols for data security.

Open Market offers free testing services and software to help Internet-based businesses and users protect themselves from potential security breaches. Open Market's Website includes a security checker so that users can test their browsers for reported security problems.

G. SECUREWARE INC.

Introduction

SecureWare Inc. has developed a Secure Web Platform to protect data and applications inside a company's own network. The security provided for network communications by Secure Sockets Layer (SSL) and Secure HyperText Transfer Protocol (S-HTTP) (Chapter V), is effective (SecureWare, 1995). However, it is not enough. Protection ends at the point where the Web server meets the Internet. Web servers and back-end systems are unprotected without Secure Web Platform. Secure Web Platform uses a three-part solution that protects data and applications from the browser to the back-end (SecureWare, 1995).

(1) The SSL security protocol (Chapter V).

(2) A secure operating system for the Web server provided by SecureWare.

(3) A comprehensive network security product for the internal network known as Hannah.

Hannah Network Security

Hannah modifies the network software on the Secure Web Platform and on the internal systems with which it communicates. It restricts access to client and server applications on the internal network and protects data. Hannah intercepts connection attempts ensuring that a user is authorized for a network connection. Hannah intercepts all network traffic between the applications to protect data integrity and encrypt it if necessary. Hannah can restrict access to applications. It can also restrict access to critical machines or server hosts. (SecureWare, 1995)

Audit Trail

The Secure Web Platform includes an audit trail mechanism built into the operating system. The system writes an audit record to an audit trail whenever a file is modified, a privilege used, an authorization granted, or an access to a file or other resources is denied (SecureWare, 1995).

Secure Web Platform Models

Most applications for the Secure Web Platform fit one of three models (SecureWare, 1995):

(1) Networks which link Web servers to an application server and then to a back-end machine.

(2) Networks which connect Web servers to an application server.

(3) Accessing a self-contained application on a Web server.

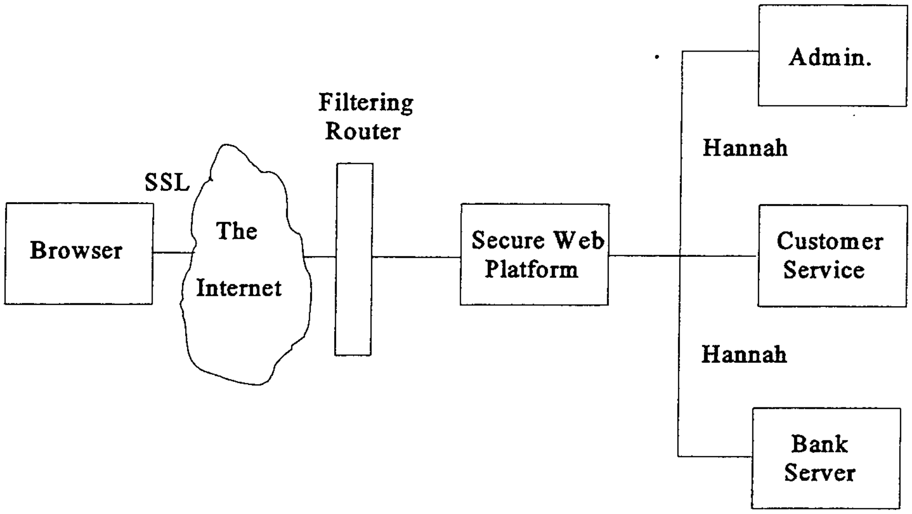


Figure 26: Model One: On-line Banking using the Secure Web Platform

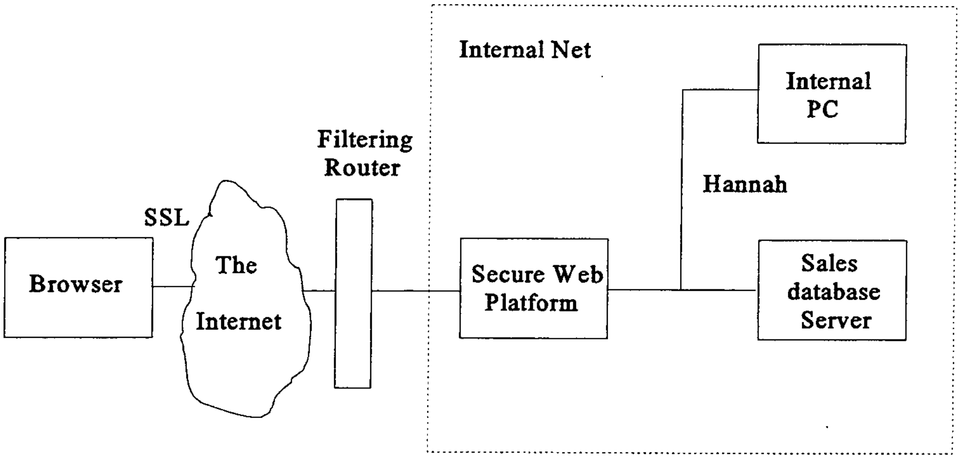


Figure 27: Model Two: Sales Application using the Secure Web Platform

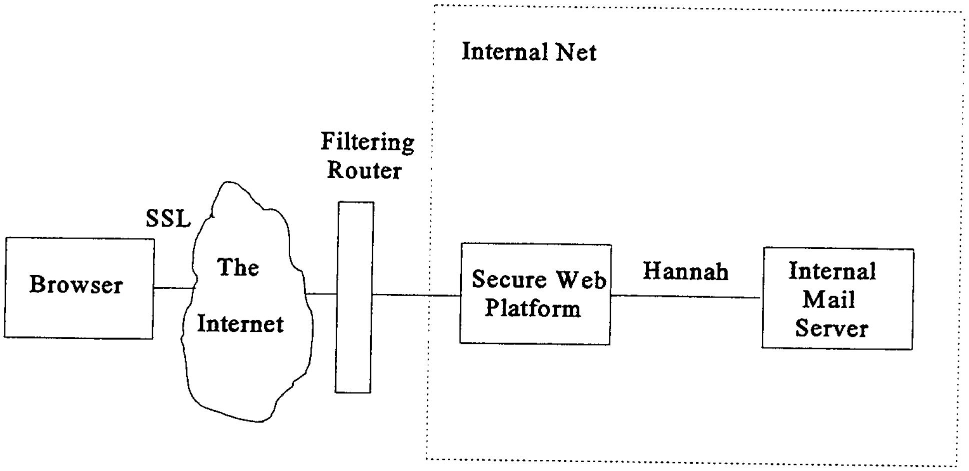


Figure 28: Model Three: Secure Web Platform's Self-Contained Support Application

Conclusion

The Secure Web Platform provides end-to-end security beginning at the Web browser. It incorporates the Netscape Commerce Server, providing SSL security protocol for client and server authentication and client-to-server encryption. The Hannah network security product authenticates administrators and other internal users, protects data and applications on the internal network and restricts access to the Web server machine and other production machines on the internal network.

H. SOUTH FLORIDA MALL (TM)

Introduction

South Florida Mall (TM) is doing business on the Internet using the Internet Commerce Security Method. The Internet Commerce Security Method was developed by Shareware in 1995. Downloading and using the method commercially is $30. South

Florida Mall merchants use this method to receive payment for their products and services. Internet data can be available to a hacker by two methods (Bodley, 1995):

(1) Intercepting data packets.

(2) Computer break-in.

South Florida Mall's Internet Commerce Security Method addresses both attacks without the use of standard encryption methods.

Internet Commerce Security Method

Consumers making a purchase on the Internet from the South Florida Mall do not send their entire credit card number over the net at once. The credit card number is divided into four groups of four digits (Bodley, 1995). The consumer chooses a four digit security code and enters it into the order form to be delivered separate from the credit card number. The two messages go to different addresses (i.e. One to the mall and one to the storefront). When the consumer enters the credit card number, simply add one of the security code digits to each of the four credit card number fields and the card number is transmitted in this altered state (Bodley, 1995).

Example:

Credit Card Number: 1234 5678 9012 3456

Security Code: 1234

Encoded Number to Send:

First Field: 1234 + 1 = 1235

Second Field: 5678 + 2 = 5680

Third Field: 9012 + 3 = 9015

Fourth Field: 3456 + 4 = 3460

Ensure the numbers in the four credit card number fields are correct and send.

Conclusion

South Florida Mall's position is that credit card use over the Internet is as safe as any other form of commerce (Bodley, 1995). Responsible consumers who use credit cards look at their monthly statements and object to charges they did not make. Responsible credit card banks also look for unusual activity and contact their customers if there is suspicious activity. Charge backs are common for illegally used credit card numbers that protect the consumer. The Internet Commerce Security Method is very simple. However, there is no protection against electronic mail interception of the encoded credit card number and the four digit security code.

I. CHECK PAYMENT SYSTEMS

1. CheckFree Corp.

Introduction

CheckFree Corp. based in Columbus, Ohio began in 1981. CheckFree is integrated with all major credit cards and the Federal Reserve Bank's electronic transfer network (Wayner, 1996). CheckFree markets its services to consumers who use CheckFree software to pay monthly bills and to corporations who need access to automated processing (CheckFree, 1996). CheckFree uses CyberCash technology to provide end-to-end Internet payment services. CyberCash's security integration allows CheckFree Wallet to create a single solution for electronic payment transactions that offers checks and credit cards (Sims, 1995).

The Concept

The average consumer can use the CheckFree software for DOS, Windows, or MacOS machines to pay monthly bills. The subscription costs $5.95 for the first 20 payments and $2.95 for each subsequent batch of ten payments (CheckFree, 1996). Paying bills using stamps is more expensive ($6.40 for 20 stamps). Actual transactions occur between bank accounts. The CheckFree application requires a voided check when opening a CheckFree account. Any money that is spent is deducted from that bank account as if a check was used.

When making a purchase on the Internet, the merchant's name and address is typed in with the purchase amount. CheckFree's computers then determine the best way to pay the merchant. Three methods are used (CheckFree, 1996):

(1) Electronic - CheckFree sends an electronic credit to your payee and electronically debits your checking account on your scheduled payment date.

(2) Electronic-to-Check - CheckFree sends the payee a check. This check is drawn from CheckFree's account. CheckFree will then debit your checking account electronically on your scheduled payment date.

(3) Laser Draft - Is just like a personal check.

The consumer schedules the payment dates with the CheckFree software. Time limits are not much of an improvement over paper (Wayner, 1996). A transaction must be entered four business days before its effective date. A stop payment order must be issued five days in advance. The four day limit is set due to the possibility of a paper check being required if the merchant does not accept electronic transfers (CheckFree, 1996).

CheckFree Wallet

CheckFree Wallet is an extension of the company's current links to the banking and credit card industry (Wayner, 1996). CheckFree Wallet was introduced in April 1995 to allow consumers to purchase goods and services from on-line merchants. The CheckFree Wallet does not require prior registration with merchants and on-line shoppers pay no fees or transaction service charges (Sims, 1995). The addition of CyberCash's technology provides consumers the ability to transmit credit card payments securely over the Internet, and merchants will receive authorization in real time. A password is used to open a consumer's CheckFree Wallet. The shipping and credit card information is protected by RSA Data Systems encryption which is used by CyberCash (CyberCash, 1996). The CheckFree Wallet browser integrates into both consumer and merchant software.

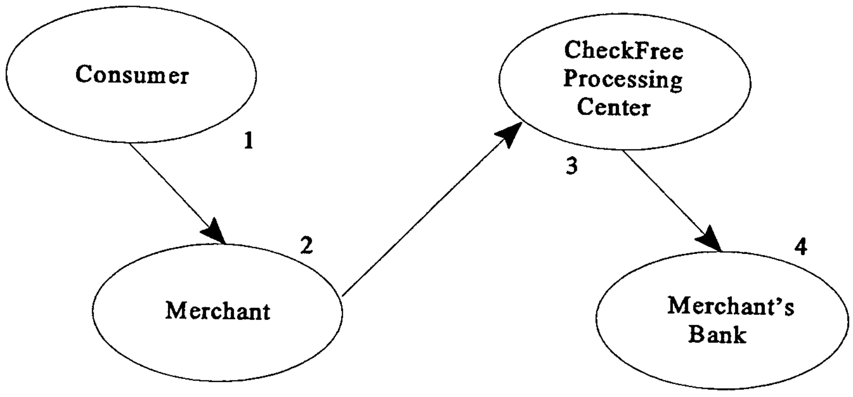


Figure 29: CheckFree Wallet Purchase Transaction (CheckFree, 1996)

(1) A World Wide Web shopper views a CheckFree-Enabled Merchant on the Internet and selects items to purchase. The encrypted payment information is sent to the merchant.

(2) The merchant adds information to the transaction and sends the encrypted transaction data to the CheckFree processing center. Upon receipt of payment authorization, an electronic receipt is created and sent to the consumer.

(3) CheckFree decrypts the transaction information, authorizes the transaction, and returns an authorization code to the merchant.

(4) CheckFree sends credit to the merchant's bank, debits the consumer's method of payment, and sends account receivable, balancing, and reconcilement reports to the merchant's bank.

Conclusion

The CheckFree system is largely used by consumers to pay bills. There is no time advantage using CheckFree. The time it takes to mail your bill payments is about the same. The risks for the consumer are minimal. Credit card companies will cover any losses more than $50. CheckFree is integrated into the banking community. However, you could perform the same transactions over the phone in the same amount of time.

2. NetCheque

Introduction

The NetCheque system is a non-anonymous system developed by Neuman and Medvinsky (Wayner, 1996). The NetCheque system imitates check clearance banking therefore, anonymity is replaced by accountability. The NetCheque system relies on the

Kerberos system (Appendix A). Trust in this system emerges from a central server that can track all major transactions if necessary (Wayner, 1996).

The Concept

A NetCheque account works the same way as a conventional checking account. The check is created by bundling the standard information (i.e. amount of the check, type of currency, name of recipient, name of bank, account number, check number). When the consumer is making a purchase, the Kerberos is called up for a ticket containing a secret key that creates a secure link to the bank (Wayner, 1996). The consumer signs the check by computing a secure hash which encrypts the secret key (Appendix A). Security is generated this way using the Kerberos model. The NetCheque system also allows the check to be endorsed using the same signature mechanism.

Conclusion

The system imitates the normal check clearing system. The principle advantage of the Kerberos system is that it uses private key encryption. The problem with the Kerberos model is that it requires each user to generate tickets to sign their checks. The tickets may expire frequently which would require a more robust, on-line environment. The Kerberos model also only creates secure channels between two parties. Therefore, there is no way for anyone else to verify signatures.

3. NetChex

Introduction

NetChex, a trademark of Net1 Inc., facilitates secure financial electronic commerce accommodating credit card and debit card payment methods. Consumers are not required to purchase additional hardware or software if they currently have Internet access. The client technology requires a base line 386 machine or higher (NetChex, 1996). NetChex is an application programming interface (API) which is easily incorporated into existing electronic data interchange (EDI) systems (NetChex, 1996). The technology allows consumers to develop unique client user interface (UI) which uses NetChex to facilitate the secure transfer of funds.

Client Software Security

The Client Software is defined as the executable modules which permit authorized users to gain access and transmit electronic checks (NetChex, 1996). NetChex does not depend on encryption to provide for security. Privacy of each transaction is provided for by applying cipher block chaining (CBC) methods to generate different private encryption keys for each transaction (NetChex, 1996).

Sixteen digit assignable signature keys provide hardware authentication. A consumer may assign a signature key to a spouse and another to a child, each with individual password protection. The signature key can be activated or deactivated at NetChex. Therefore, if a consumer suspects that a key has been compromised, NetChex will no longer accept transactions with that signature (NetChex, 1996). The NetChex client technology links itself to each consumer's personal computer when it is installed. If the software is copied to another machine, it will not work.

The security features designed into NetChex have been designed specifically to address issues of authentication, confidentiality, integrity and non-repudiation. The security methods implemented in the NetChex electronic payment system are (NetChex, 1996):

(1) Authentication: NetChex generates an integrated hardware key which incorporates characteristics specific to the PC on which the NetChex client is being installed. This key serves as the client's digital signature and is guaranteed to be unique for each member's installation.

(2) Integrity: The NetChex software verifies the integrity of each transaction it receives over the Internet through the use of cipher block chaining (CBC) methods linking each transaction to all prior transactions.

(3) Confidentiality: NetChex uses asymmetric and dynamic key encryption techniques to ensure the confidentiality of each transaction sent across the Internet. No confidential account specific information is transferred across the Internet in the processing of the transaction.

(4) Non-repudiation: The NetChex client software is copy protected to avoid the chance of unauthorized use of the software. If the client is copied or moved it will stop functioning completely rendering the application useless.

NetChex Functionality

The consumer can use the NetChex system to generate electronic checks from a PC. Prior to transmission over the Internet, the NetChex system security replaces the consumers confidential bank account information with a shadow account used to identify them to the transaction processing segment of the system. The electronic check is then transmitted across the Internet to the NetChex closed system for processing. Once received the check is verified for authenticity against the member database. The shadow account is replaced with consumer and merchant account information. The consumer is sent an e-mail confirmation of the check number and the transaction amount upon completion of a transaction. The authenticated transaction is then transferred across a private network to the appropriate banking system for processing. Once the transaction information is sent, standard banking rules are applied to complete the transfer of funds. (NetChex, 1996)

Conclusion

NetChex is designed to work within the existing bank infrastructure. NetChex does not replace the banks' role in the money transfer process. However, NetChex will be integrated in the ATM networks and in VISA/MC. NetChex offers the strongest user authentication among all of the Internet payment solutions (NetChex, 1996). Password protection and private hardware keys ensures authorize access. NetChex is a simple extension of the banking infrastructure to the Internet.

J. ELECTRONIC CASH SYSTEMS

1. DigiCash

Introduction

The DigiCash company was created by David Chaum to build the software to use his cryptographic inventions. Electronic cash by DigiCash combines computerized convenience with security and privacy (DigiCash, 1996). The structure of the DigiCash system includes both account-based money and token-based money. Each person maintains a central bank account with DigiCash. A DigiCash Wallet is assigned to each person with an account at DigiCash. Token-based digital money is subtracted from the central bank account at DigiCash for each electronic purchase (Wayner, 1996).

Security and Privacy

The security provided by electronic cash is superior to that of paper cash (Chaum, 1996). Electronic cash is digitally signed by the issuer and makes disputes over payments impossible. No mutually trusted central authority is necessary. The DigiCash software performs the necessary functions to digitally sign checks on any hardware the user has. The digital signature transforms the transaction message that is signed. Therefore, anyone who reads it can be sure who sent it (Chaum, 1996).

Privacy is achieved by an extension of digital signatures called blind signatures (Chaum, 1996). The digitally signed transaction is multiplied by a random factor generated by the consumer's PC to create the blinded signature. The consumer is anonymous. The bank and the merchant, however, receive no anonymity. Merchants do not want anonymous payments (Forrester, 1996). Merchants want to know who consumers are so they can tailor their advertising effectively.

Blinded electronic bank transactions protect the consumer's privacy, but because each transaction is simply a number, it can be easily copied (Chaum, 1996). Each transaction is checked on-line against a central list maintained by DigiCash. Verification of all transactions will prevent double spending of Ecash. However, no cryptographic protections exist (Wayner, 1996).

Ecash Functionality

A consumer making a purchase confirms the amount, merchant and description of goods. Ecash software installed on the consumer's PC transfers the correct value of

Ecash direct to the merchant. Merchants can then deposit the Ecash into their accounts. The merchant's bank receives the Ecash and is able to determine from the transaction number that it did not receive the same Ecash before. If a consumer does not have Ecash software, a DigiCash server can process the transaction. The consumer's PC needs to be operating with an HTTP server and the DigiCash server will perform everything in the same manner. (Chaum, 1996)

CAFE

CAFE is an acronym for Conditional Access for Europe (CAFE, 1996). CAFE is a project to develop electronic wallets and smart cards for Europeans to transfer cash electronically (Wayner, 1996). DigiCash is a major partner in the development of CAFE. The CAFE system is based on public key cryptography (Chaum, 1996). Digital signatures will be used to provide authentication and anonymity as in the Ecash system. CAFE is intended to unify European commerce by successfully handling all of the many different currencies (Wayner, 1996). The electronic wallets will hold value encoded in a variety of different currencies and the user may exchange the currencies by negotiating a rate. The future of the product depends on the political reaction to the system and how willing banks will be to join as partners of the project to make it a reality (Wayner, 1996).

Conclusion

Security is fundamental to electronic cash. DigiCash offers an electronic commerce solution which is being experimented with on the Internet worldwide (Chaum, 1996). However, no major banking partners are affiliated with DigiCash. Consumer anonymity is a problem for merchants trying to market their products. Merchants want to use the

Internet to build relationships with consumers and personalize their Internet storefronts.

2. Magic Money

Magic Money is an experimental system. The software was written by the Product Cipher company (Wayner, 1996). The system is similar to Ecash in that blinded digital signatures are used for authentication and consumer anonymity. Encryption is provided by Pretty Good Privacy (PGP) and digital signatures use RSA Data Systems technology. The blinded digital signature algorithms are patented by Chaum providing anonymity (Chaum, 1996). Two software application programs exist (client and server):

(1) Server - Acts like a bank. It validates, exchanges coin and maintains a list of spent coins to prevent double spending (Wayner, 1996).

(2) Client - It validates coins, maintains an electronic wallet filled with coins, and turns in coins to the bank server when they are received (Wayner, 1996).

Magic Money is secure enough to exchange coupons. However, it remains in the developmental stage.

3. NetCash

Introduction

The NetCash system used by NetBank (The First National Bank of CyberSpace) was developed by Neuman and Medvinsky (Wayner, 1996). NetCash offers consumers some anonymity. However, banks can track the spending of their customers (NetBank, 1994). NetCash payment coupons are traded via electronic mail. Consumers purchase NetCash by writing a personal check and faxing it to the NetCash Distribution Center (NetBank, 1994). The consumer may use the NetCash payment coupons to purchase information, goods or services.

Currency Server Transactions and Security

The center for activity in the NetCash system is the currency server (Wayner, 1996). The currency server exchanges NetCash coupons in two steps (Wayner, 1996):

(1) The consumer includes a hash at random and encrypts the NetCash coupons with the public key of the currency server.

(2) The currency server decrypts the incoming coupons and checks for fraud.

Encryption is provided by Pretty Good Privacy (NetCash, 1995). The security of the system also relies on one-way authentication. The currency server circulates its public key but each customer does not need to have one on file. The currency server is responsible for settling all payments. Accounts are balanced frequently and in real-time. (Wayner, 1996)

Payment Transfer

NetCash follows five basic steps to make a payment (Wayner, 1996):

(1) Two parties establish a secure channel using a published public key or an anonymous channel using Diffie-Hellman key exchange (Appendix A).

(2) The payer combines the NetCash, a session key and a session ID and encrypts them.

(3) The payee gets the NetCash and verifies the signature with the correct certificate for the currency server that generated the NetCash and sends the NetCash to the currency server. The NetCash is combined with a new key and encrypted with the public key of the currency server.

(4) The currency server checks the serial number of the NetCash to prevent double

spending. It sends the NetCash to the appropriate account for deposit. The currency server encrypts a message to be sent to payee proving that the exchange was completed.

(5) The payee decrypts the message and issues a receipt to the payer and may sign it with a digital signature as a guarantee.

Conclusion

The NetCash transaction does not require that the customer and the merchant maintain active public keys and certificates. The authenticity of the NetCash is maintained by the currency server. The NetCash could be used off-line, but the merchant would not have any protection against double spending. NetCash provides the consumer some anonymity. However, if merchants conspire with banks, they can find out who their consumers are.

4. Smart Cards

Introduction

Smart cards are unlike debit cards, which deduct money from a bank account after a purchase. Smart cards have an embedded microprocessor chip making it possible to store, retrieve and possibly manipulate data (Kezar, 1996). There are two basic types of smart cards (Kezar, 1996):

(1) Stored Value Smart Card - A simple type in which a consumer buys with a preset dollar amount and spends down. When the value is zero, it is discarded.

(2) Intelligent Smart Card - A versatile type in which the card's microprocessor can take value from a user's bank account whenever needed. An ATM could be used to add value to the card.

The intelligent smart card would be able to store not only cash balances, but also data on shopping patterns, store coupons, citizenship status, and medical history. Consumers are already seeing the benefit of the smart card, more than 30 million are being used worldwide (Kezar, 1996).

European countries have been implementing the smart card technology over the past nine years. However, smart card systems never gained much momentum in the United States until recently (Kavanaugh, 1996). Two important changes have occurred since France implemented the technology in 1982 (Kezar, 1996).

(1) Smart card technology has increased considerably and its costs have come down (Kavanaugh, 1996).

(2) The rapid increase in credit card related fraud over the past several years (Chapter IV).

a. Azteq Direct

Azteq Direct based in San Rafael, California is a provider of computer hardware and software over the Internet. Azteq Direct is offering the simpler type of smart card which is closer to a debit card for making secure transactions over the Internet. The Azteq Direct Debit Card allows consumers to order hardware, software and memory without transmitting their credit card number on-line. The account is established over the telephone and the card arrives in the mail with a personalized PIN number. (Azteq Direct, 1996)

b. Europay International

Europay International was established in 1992. Europay is a combination of the eurocheque and eurocard of the 1980's (Europay, 1996). Europay has established an

Open Terminal Architecture (OTA) for an intelligent smart card allowing consumers to gain access to cash at thousands of terminals from different suppliers (Europay, 1996). The OTA standardizes Europay's smart card and introduces microprocessing chips.

Europay and IBM teamed up in June 1995 to develop a microchip for cards using a multi-party secure open payment protocol (iKP). The product developed is known as electronic purse (Europay, 1996). Electronic purse enables monetary value to be loaded onto a chip embedded in a payment card. Europay expects to convert all cards from magnetic stripe to chip beginning in mid-1997 (Europay, 1996).

c. Mondex

Mondex is a smart card-based electronic payment system. The microprocessors contained on the Mondex smart cards can communicate securely (O'Kelly, 1996). Cash equivalent value can be stored in the cards enabling consumers purchasing power at retail stores and on the Internet. Each time a Mondex card is used, the chip on the card generates a unique digital signature. The digital signature is the guarantee that the Mondex cards are genuine (Mondex, 1996). Mondex is an alternative to cash. The microprocessor can conduct transactions without involving a third party. Mondex provides a personal balance reader permitting an individual to easily check the balance on a Mondex card. Mondex cards have global potential. They can store up to five types of currency electronically (Mondex, 1996).

d. NetFare

NetFare is a pre-paid Information Access Card that operates like a telephone access card. The NetFare Card is designed for access to desired merchandise and for downloading of data, games, forma software and single edition publications (NetFare, 1995). NetFare purchases on the Internet are low risk because the NetFare card is purchased off-line. A NetFare transaction is a four step process (NetFare, 1995):

(1) The consumer purchases a card for whatever amount is desired.

(2) The consumer presents the card to a merchant to pay for electronic information at the point of delivery.

(3) The merchant calculates the consumer's bill and checks that there is enough credit remaining on the card to pay for the product.

(4) The product is delivered to the consumer.

e. Visa

Visa has developed an electronic purse. The electronic purse is a card with a micro chip that can be used instead of cash for everything from vending machines to public transportation (Visa, 1996). The electronic purse is similar to Europay's electronic purse. The micro chip embedded in either a credit card, debit card, or stand alone card is able to store value electronically (Visa, 1996).

First Union's automated teller machines supported the Visa smart card during the 1996 Summer Olympics in Atlanta (First Union Corp., 1996). Atlanta was selected for the debut because of its large, diverse population and the international visitors expected. First Union plans to expand the Visa smart card to other cities in 1997. Diebold, Inc., based in Canton, Ohio is providing First Union's automated teller machines the upgrades to support Visa smart-card-based transactions (First Union Corp., 1996).

Conclusion

Smart cards are being developed to enable electronic funds transfer between individuals and not just between buyers and sellers. It is premature to state with certainty how many smart cards operating standards will ultimately exist. The chip card carries more information than a magnetic stripe card. And a chip card can make decisions, encrypt data and give the card holder the ability to control who has access to the data carried in the card.

K. MICROPAYMENT SYSTEMS

Introduction

Micropayment systems support low cost purchases of information on the Internet. Speed and cost of processing payments are critical factors in assessing a protocol's usability (Baker, 1996). Fast user response is essential if consumers are to be encouraged to make a large number of purchases. Servers are required to have the capacity to deal with fluctuations in demand. Not everyone everyday will want to download a newspaper. However, if a major news story is being reported, the demand will dramatically increase (Abadi, 1995). On-line services providing newspapers, magazines, reference works, and stock prices all have individual items that could be inexpensive if sold separately. The ability to purchase inexpensive individual items would make these services more attractive to casual users on the Internet (Abadi, 1995). The following are statistics from the 1994 American Information User Survey on how much Internet user households are willing to pay for electronic publishing services.

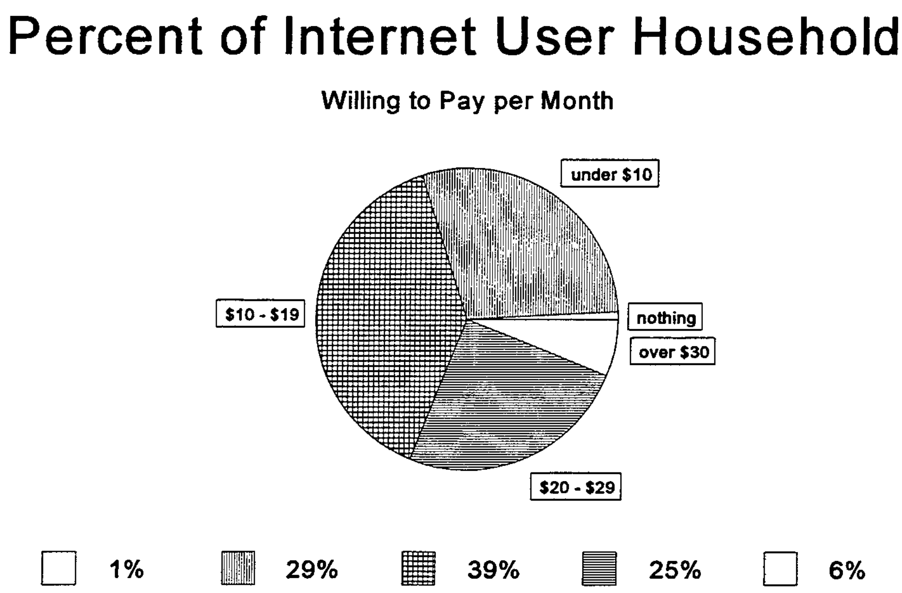


Figure 30: American Information User Survey, 1994

1. Micropayment Protocols

a. Micro Payment Transfer Protocol (MPTP) V0.1

MPTP is used for low value transfers between parties for the purchase of information on the Internet. MPTP involves three parties (Baker, 1996):

(1) A customer (making the payment)

(2) A vendor (receives the payment)

(3) A broker (a financial intermediary who keeps the accounts for both parties)

Presently only a single broker model is considered. However, the protocol does not restrict the broker to use of a single server (Baker, 1996).

MPTP uses shared secret and public key based digital signature schemes. Choice of algorithms and key length is left to the parties involved (Baker, 1996). A considerable degree of flexibility for establishing a payment policy is allowed by MPTP. It supports the use of multiple payment encounters to optimize processing time which shortens payment time (Baker, 1996).

Certificates bind a public key to an account number under the public key of the broker (Baker, 1996). The broker's public key is known to all parties. The problem with certificates is that they expire and need to be re-issued. It becomes difficult to track credit risks or permit certificates to be valid for long periods of time (Baker, 1996). The broker in this protocol takes all risk of non-payment. However, MPTP permits the broker to transfer this risk to the vendor by refusing to guarantee payment (Baker, 1996).

MPTP is a protocol for Internet purchases of information. The protocol is also suitable for use as an access control or for resource allocation. An important characteristic which a micropayment scheme must satisfy is to permit access to both small and large publishers. Use of public key signature screening makes it economic for use by small publishers. (Baker, 1996)

b. Millicent Protocol

Millicent is a secure protocol designed to support information purchases over the Internet costing less than a cent. It is based on decentralized validation of electronic cash at the vendor's server without any additional communication, expensive encryption, or off-line processing (Abadi, 1995). The key innovations of Millicent are its use of brokers and of scrip. Brokers take care of account management, billing, connection maintenance, and establishing accounts with vendors. Scrip is digital cash that is only valid for a specific vendor. The vendor locally validates the scrip to prevent customer fraud, such as double spending (Abadi, 1995).

Security is achieved by using scrip and the brokers who sell it. Scrip represents an account a customer has established with a vendor. The balance of the account is kept as the value of the scrip. When the customer makes a purchase with scrip, the cost of the purchase is deducted from the scrip's value and new scrip (new account balance) is returned as change. When the customer has completed a series of transactions, the scrip may be cashed in closing the account with the vendor. (Abadi, 1995)

Brokers serve as accounting intermediaries between customers and vendors. Customers enter into long term relationships with brokers, similar to an agreement with an Internet service provider (Abadi, 1995). Brokers buy and sell scrip as a service to customers and vendors. Security and privacy is added to the Millicent protocol using shared secrets between parties and using the secret to set up secure communications using encryption (i.e. DES, RC4 or IDEA) (Appendix A).

Initial implementation of Millicent for transactions across a network using TCP/IP has been efficient for purchases less than a cent (Abadi, 1995). The Millicent protocol price range covers most print and information services that will be available in an on-line format (Abadi, 1995). A Millicent-based Internet service is currently being developed.

c. PayWord and MicroMint Protocols

PayWord and MicroMint are micropayment protocols developed by Rivest and Shamir (Abadi, 1995). Inspired by the Millicent Protocol, their goal is to minimize the number of public key operations required per payment using hash operations (Rivest, 1996). PayWord is a credit-based scheme. Authentication is performed using public key cryptography (Appendix A). PayWord is optimized for sequences of micropayments. However, it is secure and flexible enough to support larger payments (Rivest, 1996).

MicroMint is designed to eliminate public key operations totally. Security is sacrificed for speed (Rivest, 1996).

(1) PayWord: The PayWord user establishes an account with a broker, who issues a digitally signed PayWord certificate containing the broker's name, the user's name, the IP address, and the expiration date (Rivest, 1996). The certificate has to be renewed monthly by the broker, who ensures the consumers account is in good standing. The certificate authorizes the consumer to make PayWord transactions (Rivest, 1996). PayWord does not provide consumers anonymity. However, some privacy is provided since there is no record kept as to which documents were purchased (Rivest, 1996). PayWord is summarized by the following (Rivest, 1996):

(1) The broker is required to sign each certificate and perform one hash function application per payment. The broker stores copies of consumer certificates and maintains accounts for consumers and vendors.

(2) The consumer is required to verify their own certificate and perform one hash function application per payment. The consumer stores their own secret key.

(3) The vendor verifies all certificates and performs one hash function application per payment. The vendor stores all purchases and last payment received per consumer each day.

(2) MicroMint: MicroMint is designed to provide reasonable security at a very low cost. MicroMint uses no public key operations at all (Rivest, 1996). MicroMint coins are produced by a broker who sells them to consumers. The broker issues new coins at the beginning of each month and the coins are only valid for that month. Unused

coins are returned to the broker at the end of the month to purchase new coins. MicroMint coins are represented by hash functions (MD5 and DES) (Rivest, 1996). MicroMint is not anonymous. The broker can detect a coin that is double-spent and can identify which vendors received them. It does not use digital signatures. Therefore, it would be difficult to legally prove who is guilty of duplicating coins (Rivest, 1996).

2. Micropayment Companies

a. Clickshare Access and Payment Service

Clickshare provides consumers with a digital calling card using private key encryption allowing them to log in once and charge purchases from publishers at several Web sites to a single account (Clickshare, 1996). The Clickshare micropayment service also provides multi-site user authentication. Clickshare enables the anonymous tracking of individual users as they jump among unrelated Internet sites. The smallest transaction the system settles is ten cents. The Clickshare system remains in the developmental stage (Clickshare, 1996).

b. CyberCash

Please see Chapter VI section C.

c. First Virtual Holdings Inc.

Please see Chapter VI section D.

d. Infosafe Systems Inc.

Infosafe customizes and markets secure electronic distribution systems for digital information, video, graphics and software direct to end users from any electronic source. The company is currently testing its proprietary solution using DES to conduct secure electronic financial purchases of information on the Internet (Infosafe, 1996). The consumer benefits for Infosafe subscribers will be (Infosafe, 1996):

(1) Greater access to information (24 hours daily)

(2) Lower cost (pay for information used)

(3) Cost tracing (track all transactions)

(4) Internal Usage Controls (Manage information spending)

The Infosafe system allows subscribers to search the library contents free, perform product comparisons and test demos of products offered through the system (Infosafe, 1996).

e. ZipLock

ZipLock is an automatic distribution, payment system providing instant 24 hour access to digital content, including software, publications and information services. Developed by Astoria Software, ZipLock acts like an electronic safe-deposit box connecting the customer directly to the credit card processing company transferring funds to merchants for purchases (Astoria, 1995). The ZipLock system uses encryption technology from RSA Data Security, Inc. Credit card authorization occurs without the merchant seeing the customer's credit card. ZipLock uses a secure, direct modem connection between the customer and the credit card processor (Astoria, 1995). ZipLock has been in use since late 1995.

L. ON-LINE BANKING SYSTEMS

Introduction

Commercial banks have shown only a limited interest in the Internet (Crede, 1996).

Some banks argue that the openness of the Internet makes it unsuitable for handling transfers of information relating to money and security would be almost impossible to implement (Crede, 1996). However, secure Internet payment systems are being developed and implemented by many companies (i.e. Visa, MasterCard and Netscape) and banks are starting to notice and rise to the challenge (Bank Administration Institution (BAI), 1995).

1. BankAmerica Corp.

BankAmerica Corp. is the second largest banking company in the Untied States with assets of $227 billion at second quarter 1995 (BankAmerica Corp., 1996). Bank of America has announced in June 1996 an on-line HomeBanking service which is available to consumers and small businesses through America Online and the Internet (BankAmerica Corp., 1996). Customers who sign up for HomeBanking are charged a $6.50 monthly fee. However, this fee can be waived if customers have a Versatel checking account with direct deposit (BankAmerica Corp., 1996). HomeBanking on the Internet requires users to have Netscape Navigator 1.22 or higher for Windows and 1.12 or higher for Macintosh or UNIX systems. HomeBanking offers the following Internet features (BankAmerica Corp., 1996):

(1) Quick Balance: This feature gives current balances for all HomeBanking accounts.

(2) Account Information: This feature allows customers see and download all posted activity for each HomeBanking checking accounts for the current and the previous two statement periods. Customers can also review recent payments and transfers and see details of specific transactions or cancel any future payments. Customers will know

when a direct deposit has arrived or when a check has cleared.

(3) Bill Payments: Customers can pay all of their bills on-line to individuals as well as businesses. Bill scheduling is offered up to one year in advance and have payments arrive precisely on time.

(4) Transfer Funds: This feature moves funds easily between the Bank of America checking and savings accounts that are linked to HomeBanking and even advance funds from credit card accounts to other accounts.

(5) Customer Service: HomeBanking provides secure e-mail access to customer service.

(6) Financial Analysis and Planning: HomeBanking provides a software program (Managing Your Money) that gives customers analytical and planning capabilities.

(7) Downloading and Importing: HomeBanking has a built-in Quicken Interchange Format (QIF) which is the industry standard for information exchange between personal money management software. This feature allows customers easily download the current session or the full detailed checking account activity into a personal spreadsheet or a personal money management program.

Secure e-mail is provided by Privacy Enhanced Mail (PEM) or the Multipurpose Internet Mail Extension (MIME). The security technology employed uses public-private, or asymmetric, key technology patented by RSA Security Inc. (BankAmerica Corp., 1996).

Bank of America has joined Netscape Communications Corp. providing businesses with a secure means for electronic commerce. Bank of America's payment service will allow business conducting Internet electronic commerce to accept Visa, MasterCard, Discover Card, Diners Club, Carte Blanche, JCB Card or American Express card on-line (Netscape, 1996). The service will be based on Netscape Communications's Netscape Commerce Server software with additional transaction processing capabilities to handle payment processing. Customers may create their own Internet storefront using the Netscape Commerce Server. Bank of America is the only bank offering customers so many choices for accessing a home banking service (BankAmerica Corp., 1996).

2. Intuit Inc.

Intuit Inc. plans to offer banking via the Internet with participating financial institutions using security provided by RSA Data Security by late 1996 (Intuit Inc., 1995). Intuit is developing both a general interface for Internet banking and a customized version that will integrate Netscape Navigator. Intuit's new interface will include security features based on RSA Data Security encryption. Triple DES session keys will be exchanged using 1024-bit RSA and will encrypt all banking data transmitted between the customer and their financial institution including PIN's (Intuit Inc., 1995).

Each financial institution will decide pricing and servicing packaging for these new services. Financial institutions have the potential to reach more than 12 million people who use Quicken or America Online (AOL) and about one million who use other Intuit supported interfaces (Intuit Inc., 1995). Intuit has delivered electronic banking to customers of 22 participating financial institutions via Quicken since October 1995 and announced a strategic alliance with AOL to give subscribers access to on-line banking in November 1995 (Intuit Inc., 1995). The latest financial institutions to join Intuit Inc. are Alex. Brown & Sons, BankAtlantic, Bank of Stockton, Charles Schwab & Co. Inc., Commerce Bancshares, Commercial Federal Bank, Dreyfus Services Corp., Fidelity Investments, First Hawaiian Bank, First Union Nation Bank, Laredo National Bank, Mellon Bank, PNC Bank, Republic National Bank of New York and Signet Bank (Intuit Inc., 1996).

3. Security First Network Bank

Security First Network Bank (SFNB) is the world's first Internet bank which provides software for other banks and financial institutions allowing them to offer on-line banking services (Security First Network Bank, 1996). SFNB became the world's first Internet bank on October 18, 1995 and within six weeks had more than 1,000 applications for checking accounts from people in 40 states, Japan, Australia and Canada (Northwestern, 1996). Customer accounts can be accessed from any computer with a secure Internet browser (i.e. Netscape Navigator).

Security First uses several layers of technology to ensure the confidentiality of its transactions across the Internet. Netscape's Secure Sockets Layer (SSL) is used to provide privacy for the data flowing between the browser and the bank server (Chapter V). The bank is protected by a system of filtering routers and firewalls which form a barrier between the outside Internet and the internal bank network (Security First Network Bank, 1996). Security First uses SecureWare's SecureWeb Platform as part of its architecture for security within the bank itself (Security First Network Bank, 1996). The system meets the stringent B-1 level security classification which the U.S. government reserves for highly sensitive military systems (Lafferty, 1996).

Security First Network Bank is made up of two distinct parts. The Information Server is the area potential customers use to learn about the bank and its services (Security First Network Bank, 1996). Once a customer decides to open an account, an encrypted registration form is sent to the Bank Server, which contains the actual banking applications (Security First Network Bank, 1996). The bank verifies the account information and creates a new account for the customer. Customers communicate with the bank using their World Wide Web browser.

Security First Network Bank has achieved levels of data protection never before used in a commercial operation (Security First Network Bank, 1996). Consumers can be certain that as Internet security technologies evolve, Security First will continue to test, evaluate and implement those that might be beneficial (Security First Network Bank, 1996).

4. Wells Fargo Bank

Wells Fargo provides customers with encrypted on-line banking sessions. Customers' banking session data is encrypted using Netscape's Secure Sockets Layer (SSL) protocol (Chapter V). Wells Fargo uses a thorough authentication process during enrollment to ensure that the customer is the only one who can access their account (Wells Fargo, 1996). Customers must enter their Social Security Number and a unique on-line password to begin a banking session. Wells Fargo only sends a partial account number over the Internet to protect the full account number (Wells Fargo, 1996). Information is also protected by an automatic sign-off capability terminating the session if the system is not actively in use for more than ten minutes (Wells Fargo, 1996). Wells Fargo Internet banking features are (Wells Fargo, 1996):

(1) View current balances on checking, savings and credit card accounts.

(2) View cleared checks and deposits or withdrawals posted.

(3) Transfer funds between accounts.

(4) Examine credit card charges and payments.

(5) Download account transaction information to personal financial software.

Customers can pay anyone (individuals or businesses) and schedule payments in advance from anywhere using a personal computer, a touch tone phone or a Wells Fargo Automatic Teller Machine (ATM). Recurring payments can be set up weekly, monthly or annually. Payments can be set up immediately and be changed or cancelled until the day it is due. Customers have unlimited payment options for $5.00 per month. (Wells Fargo, 1996)

VII. CONCLUSION

Electronically based payment systems are nothing new. These payment systems have been in operation since the 1960s and have expanded rapidly as well as grown in complexity. However, these payment systems are mostly proprietary closed networks developed by the banking industry for large value payment transactions. The rapid growth of the Internet has created new commercial opportunities for networked commerce. Recent developments in secure payment systems could permit the creation of a new cost-effective global payment system for low value payments. Internet payment systems will provide opportunities for the creation of completely new sets of national and global trading partners for small and medium businesses.

The creation of an industry standard is crucial to widespread acceptance of financial transaction methods over the Internet. Several companies have developed financial transaction systems and are competing for consumer loyalty. Software and data security companies aggressively marketing their products, often tap into the consumers' concern about security issues. Consumer confidence will be gained with the acceptance of an industry standard backed by brand names they can trust. The Secure Electronic Transaction (SET) payment method due in late 1996 may provide the industry with the standard needed. SET has been aggressively developed by a strategic alliance of reputable companies in the industry including: Visa, MasterCard, Microsoft, IBM, and Netscape.

The concern about security of financial transactions on the Internet is more of a perception than it is a reality. Industry experts agree that financial transactions over the Internet are safer than conventional transaction methods. It is more dangerous to hand a credit card to a clerk at a retail store or a waiter at a restaurant, than it is to transmit your credit card number over the Internet. The most common credit card transaction is the "card-not-present" method. This method allows the merchant to take the credit card number over the phone without seeing the credit card. The opportunity for fraud with this method is great. Even when the consumer physically presents their credit card to a merchant, the number is sent over a telephone line at 1200 baud in clear ASCII. The financial transaction methods available for use over the Internet and analyzed in this thesis are more secure than conventional transaction methods. Credit card numbers are never sent over the Internet in the clear in these systems, and a majority of the methods studied use some form of encryption.

It has been established that the financial transaction systems studied are secure. However, the barrier to electronic commerce is the consumer perception that these methods are not secure. These fears must be eliminated and the confidence of the consumer must be gained in order for electronic commerce to reach its full potential. The shopping experience must be convenient for the consumer, and they must feel that there is a value-added benefit of shopping online. Merchants must take advantage of the two-way medium of the Internet to establish one-to-one customer relationships.

The ability of the Web to amass, analyze, and control large quantities of specialized data can enable comparison shopping and speed the process of finding items. Search engines tailored to consumer preferences will enable this comparison shopping.

Consumers must have access to the Web in order to shop. Convenience of access is at the core of the adoption of any technological application and will determine its success. The penetration of home personal computers has exceeded one-third and modem access is 19%. The penetration of home personal computers and convenience of access will level the demographic profile of an Internet user and render a more representable cross-section of society. This representative profile and increased access will lead to increased Internet sales.

Sophisticated encryption and authentication technology has been viewed as the crucial enabling technology for electronic commerce over the World Wide Web. However, it must be remembered that a chain is only as strong as its weakest link; therefore, when implementing a system for the protection of data, both organizational and technical aspects must be considered. Merchants must have a security plan providing end-to-end protection. The best security product in the world can be compromised if not implemented correctly.

The Department of Defense has been keen to emphasize security and strategic benefits through streamlining and integrating its business processes. It follows, then, that the DOD and the entire federal government has a stake in the Internet's capability to process secure financial transactions. This is particularly true where the DOD or other agency is receiving payments, making payments or communicating sensitive documents such as bids. This need for communication security will grow as more agencies and commands solicit bids from a geographically broad market of vendors through home pages on the World Wide Web.

APPENDIX A

Cryptography is the science of keeping messages secret. Once used almost exclusively by the military, the art of cryptography has become a valued asset in keeping data and computer systems secure (Ylonen 1996). The goal of any cryptosystem is to maintain four essential elements:

(1) secrecy

(2) authenticity

(3) integrity

(4) non-repudiation.

A cryptosystem provides secrecy by ensuring that an unauthorized source cannot derive plaintext from the encrypted ciphertext or given the ciphertext and the corresponding plaintext, the key used for encryption cannot be derived. Authenticity is realized when the source of a message can be validated and no replays of a previous message can be sent. Integrity is achieved by prohibiting the insertion, deletion, or modification of data. Cryptosystems provide non-repudiation when the sender cannot deny the transmission of data. A description of the most common algorithms used in cryptography are provided below.

Symmetric (Private) Key Encryption

The oldest and best-known forms of encryption use private keys that are known to both the sender and receiver. The key lengths of these systems vary in size, but all symmetric key systems use the same private key for encryption and decryption when sending and receiving data. Several software products use symmetric key cryptography for fast bulk encryption. The following algorithms implement symmetric key cryptography.

Data Encryption Standard (DES)

The most common symmetric key algorithm used today is still the United States Government's Data Encryption Standard (DES). This algorithm was initially developed by IBM in the 1970's and reviewed by the National Security Agency before being released to the public. The system was adopted by the National Institute of Standards and Technology as the standard for nonclassified U.S. government data in 1976 and has been recertified by the NIST every five years; last recertified in 1993 (Wayner 1996). DES was approved by the American National Standards Institute (ANSI) as a private-sector standard in 1981 (Hartmann 1996). Today, DES forms the basis of several ANSI standards for financial institutions and is used in numerous applications world-wide.

DES is a block encryption cipher. It uses a 64-bit block with a 56-bit key. There are two block encryption modes commonly used with DES. Encryption Code Book (ECB) is the simplest of the two modes. ECB encrypts 64-bit blocks independent of all other 64-bit blocks. The advantage of ECB is that only blocks in error need to be retransmitted, yet the disadvantage of this method is that identical plaintext blocks produce identical ciphertext blocks given the same key. The second and most commonly used mode is Cipher Block Chaining (CBC). This method takes each 64-bit plaintext block and XORs with the previous ciphertext block before being encrypted with the DES key. The XOR takes bit inputs (0 or 1) from the plaintext block and previous ciphertext block and performs the logic operation exclusive OR as illustrated below:

Inputs		XOR
0	0	0
0	1	1
1	0	1
1	1	0

Thus the encryption of each block depends on previous blocks and the same 64-bit plaintext block can encrypt to different ciphertext depending on its context in the overall message (RSA 1995).

The DES algorithm encrypts data by repeating a basic scrambling in 16 rounds. Each round uses a different key derived from the single key provided by the user. The keys are derived from a key scheduling algorithm which is completed before enciphering or deciphering the information. The cipher text message is decrypted by applying the keys in the reverse order used to encrypt the message.

Triple DES

DES has never been broken, despite the efforts of many researchers over many years. The longer a cryptography method withstands the scrutiny of the public, the more secure the method is considered. However, it has been estimated that with today's computing power a customized machine built to perform an exhaustive search of all possible keys in seven days could be built for $1 million (Lieu 1995).

A powerful technique for improving the security of DES is triple encryption. Triple

DES encrypts each message block under three different DES keys in succession. This technique overcomes the main weakness of DES, it's small key size. Triple encryption is thought to be equivalent to doubling the key size of DES, to 112 bits, and should prevent decryption by an enemy capable of single-key exhaustive search (Merkle-Hellman 1981). The main disadvantage of triple DES is that increased security has a cost of tripling the computational effort which results in a reduced speed and possibly an increase in processing hardware.

IDEA (International Data Encryption Algorithm)

IDEA was developed in the early nineties by Lai and Massey (Hartmann 1996). It is a block cipher which uses 64-bit blocks but a 128-bit key. IDEA was developed as a replacement for DES. Although the key size is twice as long as DES, IDEA has shown roughly twice the speed of DES in software implementations (Hartmann 1996). The fundamental innovation in the design of this algorithm is the use of table look-ups and substitution tables used in systems like DES have been dispensed with. Instead, the algorithm uses the operations from three different algebraic groups. The encryption process consists of eight rounds of encryption steps followed by an output transformation.

IDEA has been designed to overcome both brute force (exhaustive search) and intelligent attacks. It has been under public scrutiny for over four years and no weaknesses have been discovered. Ascom, the Swiss telecommunications company who owns the rights to the algorithm, is so confident IDEA will not be cracked it has set a reward for cracking the algorithm. IDEA is one of the best-known new publicly available symmetric key algorithms. A considerable number of banks, international corporations and government agencies have obtained site licenses and are using IDEA for protecting communications. PGP which stands for "Pretty Good Privacy" invented by Phil Zimmerman also uses the IDEA algorithm in it's software package used for encrypting data files, signing files electronically, and key management.

RC4

RC4 is a symmetric key algorithm developed by Rivest of RSA Data Security, Inc. It is a stream cipher, which means that it is basically a pseudo-random number generator where the number generated is XORed with the data stream. This makes RC4 ten or more times as fast as DES in software applications. However, since RC4 is a symmetric stream cipher, it is important that the same key never be used to encrypt two different data streams. It is useful in situations where session keys for each new message are produced.

RC4 USES a variable key length up to 2048-bits. Most applications use a 40-bit key length, allowing them to export their product under current U.S. State Department export laws. DES, with a key length of 56-bits, is rarely approved for export other than to foreign subsidiaries or overseas offices of U.S. companies. An agreement between the Software Publishers Association(SPA) and the U.S. government gives RC4 special status by means of which the export approval process is simpler and quicker than the usual cryptographic export process. The stipulation is that the key length must not surpass a length of 40-bits (RSA 1995).

Security of RC4 can be strengthened by adding a 40-bit string called a salt. The salt can be used to thwart attackers who try to precompute a large look-up table of possible encryptions. The salt is appended to the encryption key, and this lengthened key is used to encrypt the message; the salt is then sent, unencrypted, with the message(RSA 1995). RC4 is widely used by developers who wish to export their products. It is also used domestically for superior symmetric key encryption (2048-bit) to DES for applications like bulk encryption. Products such as Lotus Notes and Netscape Secure Commerce Sever use the RC4 algorithm.

SkipJack Algorithm/Clipper Chip

The Skipjack algorithm was designed by NSA as a replacement for the aging DES algorithm. The Skipjack algorithm is classified, therefore few details are known. It is known that the Skipjack algorithm is contained in a hardware device known as the Clipper Chip. A consequence of Skipjack's classified status is that it cannot be implemented in software, but only in hardware by government-authorized chip manufacturers.

The Skipjack algorithm uses an 80-bit key to encrypt 64-bit blocks of data, thus it is believed to be more secure than DES which uses only a 56-bit key. It is a symmetric key system and uses the same key for decryption. It is known that the algorithm uses 32 rounds to scramble data. Another advantage is that the algorithm cannot be reverse engineered from the Clipper Chip. The decision to classify the algorithm has drawn criticism from experts in the field. They suspect that either the algorithm is insecure or that there is a trapdoor built into the algorithm (RSA 1995).

The concept of a government designed standard such as the Clipper Chip has privacy advocates up in arms. The Clipper Chip attempts to balance the needs of law-enforcement agencies with industry and private individuals by using escrowed keys. The idea is that communications could be encrypted, but the keys would be maintained by two or more third party private escrow agencies. This way personnel and industrial communications would be kept secret, yet law-enforcement agencies could still tap suspected criminal communications with the appropriate court order (Lieu 1995). Privacy advocates are concerned that government and law enforcement agencies will be able to backdoor escrow agencies. They are also questioning how such agencies will be established and who will regulate them.

Asymmetric (Public) Key Encryption

The concept of public key cryptography was introduced in 1976 by Diffie and Hellman and later refined by Rivest, Shamir, and Adleman in 1977 (RSA 1995). The private key systems worked well in small networks. As a network expands, the secure exchange of secret keys becomes increasingly expensive and unwieldy. An additional drawback to the private key system is the requirement of sharing a secret key. Each person must trust the other to guard the pair's secret key, and reveal it to no one. Essentially, this means that communication can only take place between people with some kind of prior relationship. Authentication and non-repudiation are also issues with the private key systems. Shared secret keys prevent either party from proving what the other may have done. Either can modify data and be assured that a third party would be unable to identify the culprit. The same key that makes is possible to communicate securely could be used to create forgeries in the other user's name (Verisign 1996).

These problems were addressed by Diffie and Hellman in 1976 when they proposed a method of exchanging secrets without exchanging secret keys. Public key cryptography uses key pairs, a public key and a private key. One key is used to encrypt the data while the other key is used to decrypt the data. The important feature is that the key used to encrypt the data cannot be used to decrypt the data. In a public-key system, one simply publishes their public key and keeps the private key secret. If someone wants to send a message that can't be read by anyone else, they look up the public key of the person and use it to encrypt the message. Only the person with that key can use it to decrypt the message (Wayner 1996). Hence public key cryptography solves one of the most vexing problems of all prior cryptography: the necessity of establishing a secure channel for the exchange of the key. To establish a secure channel one uses cryptography, but private key cryptography requires a secure channel.

The key lengths used in public key cryptography are usually much longer than those used in private key ciphers. The problem is not guessing the right key, but deriving the matching secret key from the public key. It has been estimated that for the RSA cryptosystem, a 256 bit modulus is easily factored by ordinary people. A key length of 384 bits is said to be susceptible to university research groups or companies and 512 bit key is within reach of major governments. It takes a 768 bit key or more to be safe in the long term (Ylonen 1996).

Digital Signatures and Certification Authority

A digital signature is analogous to a written signature. It uniquely and undeniably identifies the originator of a message. A user digitally signs a message which a recipient can verify. The signature has to be difficult to forge, yet easy to verify. This process is accomplished by signing a message with the private key. This ensures that the message could only have come from the private key holder, yet anyone could verify that the message was genuine.

Since public keys can be published in any directory without exchange through a prearranged trusted source, the issue of public key legitimacy surfaced. The argument is that anyone can masquerade in a computer network as a legitimate user receiving sensitive documents at a false account. There are currently two solutions to the certification issue: building a 'web of trust', and setting up official key issuing authorities. The web of trust works through personal recommendations. The public key is signed by other people who can vouch for the user. If the recipient trusts one or more of the people, then the message can be considered legitimate. Phil Zimmerman's PGP uses this method (Lieu 1995). The alternative is the central issuing authority. This organization creates a kind of digital passport or credential. The Central Authority (CA) digitally signs the user's public key, this is referred to as the Digital ID. Every time someone sends a message, they attach their Digital ID to verify the author's public key is authentic, then uses the public key to verify the message itself. Through the use of Digital ID's, an authentication chain can be established, allowing for convenient public key registration and certification in a distributed environment (Lieu 1995).

Hash Algorithms

Hash algorithms are used in conjunction with digital signatures for efficiency and authenticity. The hash algorithm produces a fixed-length string from a variable input. The fixed-length string varies in size depending on the algorithm. This string is called the message digest. The shorter message digest is then encrypted using the private key of the sender, turning it into a digital signature. Since the hash algorithm is faster than the public key signing function, it is more efficient to compute the digital signature using a message digest, which is small, than using the entire document.

The hash algorithm has the added benefit of providing data authentication. The strength of a hash algorithm rests in the one-way nature of the algorithm. It is easy to compute a hash value for a given input, but it is extremely difficult to derive an input which will produce a specified hash value. The recipient of a message decrypts the digital signature and then recalculates the message digest. The value of the newly calculated message digest must match the digest found in the digital signature exactly. Any deviation between the two message digest, whether intentional or unintentional, indicates the message has been altered and a problem exists.

MD4, MD5, and SHS

MD4, MD5, and SHS are the most recognized hashing algorithms in use today. MD4 and MD5 are algorithms developed by Ron Rivest of RSA Data Security, Inc. MD4 and MD5 produce 128 bit digests and there is no known attack faster than an exhaustive search. MD5 is more secure against attack than MD4, but it is also 33 percent slower. MD4 can also be modified to supply a 256 bit digest. MD5 is the most commonly used of the RSA Data Security, Inc. algorithms (RSA 1995).

The Secure Hash Standard (SHS) is a hash algorithm proposed by NIST and adopted as a U.S. government standard. It is designed for use with the U.S. government's proposed Digital Signature Standard. SHS is based on MD4. The algorithm produces a

160 bit hash value which works well with the 160 bit modulus used by DSS. Due to the 160 bit length of SHS it is considered more secure than MD5, but is also 25 percent slower due to the additional key length (Wayner 1996).

RSA

RSA is a public key cryptosystem invented in 1977 by Rivest, Shamir, and Adleman while at MIT (RSA 1995). It can be used for both encryption and signing. It is generally considered secure when sufficiently long keys are used. The security of RSA is predicated on the assumption that factoring large integers is difficult. The RSA algorithm has endured over 15 years of scrutiny, yet there has never been an explanation of a reliable method to attack the RSA system (Wayner 1996).

RSA takes two large prime numbers, p and q, and finds their product $n=pq$ which is called the modulus. A number is then chosen, e, less than n and relatively prime to $(p-1)(q-1)$. The inverse,d, mod $(p-1)(q-1)$ is found, which means that $ed =1 \bmod (p-1)(q-1)$. e and d are called the public and private exponents, respectively. The public key is the pair (n, e); the private key is d. The factors p and q must be kept secret or destroyed (RSA 1995).

RSA is used for privacy (encryption) as follows: Alice wants to send a private message, m, to Bob. Alice creates the ciphertext, c, by exponentiating: $c = m^e \bmod n$, where e and n are Bob's public key. To decrypt, Bob also exponentiates: $m = c^d \bmod n$, and recovers the original message, m; the relationship between e and d ensures that Bob correctly recovers m. Since only Bob knows d, only Bob can decrypt.

RSA is used for authentication as follows: suppose Alice wants to send a signed document, m, to Bob. Alice creates a digital signature,s, by exponentiating: s = m^d mod n, where d and n belong to Alice's key pair. She sends s and m to Bob. To verify the signature, Bob exponentiates and checks that the message, m, is recovered: m = s^e mod n, where e and n belong to Alice's public key (RSA 1995).

RSA is not a replacement for symmetric key algorithm, but a supplement to them. RSA is most widely used in a protocol referred to as a digital envelope. This protocol uses symmetric key cryptography for bulk encryption of the message and then encrypts the symmetric key using RSA cryptography. This method ensures the fastest possible encryption without the problems associated with key management of private keys. RSA can be used for plaintext encryption, but this use of RSA is extremely inefficient when compared to symmetric key systems like DES. DES is estimated to be at least 100 times faster than RSA in software applications and between 1,000 and 10,000 times as fast in hardware applications (RSA 1995).

Diffie-Hellman

Diffie-Hellman was the first public key cryptographic technique published. The security of Diffie-Hellman relies on the difficulty of the discrete logarithm problem (which is believed to be computationally equivalent to factoring large integers). It is primarily used for public key exchange for use in other private key crytosystems (Unruh 1996). The system requires the dynamic exchange of keys for every sender-receiver pair and in practice, this exhange of keys occurs during every communications session. This two-way key negotiation is useful in further complicating attacks, but requires additional communications overhead. The Diffie-Hellman method also has no way to produce digital signatures (Unruh 1996).

Digital Signature Standard (DSS)

DSS is a signature-only mechanism endorsed by the U.S. government. This system is composed of the Secure Hash Standard (SHS) and the Digital Signature Algorithm. The SHS is described above. The security of DSA is based on the discrete log problem. This means that given a message, m, and a value, a, it is easy to compute m^a mod p where p is a prime number. If given another value n, it is difficult and certainly infeasible ato discover a value of, a, such that m^a mod p = n. That is, it is hard to take the discrete log of n (Wayner 1996).

The details of the DSA are unknown except that the modulus is 160 bits and the key size can vary from 512 to 1024 bits. A message is digitally signed the same as in any public key system. The message is first hashed with the SHS and then the DSA is used to sign the message. Encryption for key exchange is not possible with this system. DSS has not be released to the public for critisism, so the overall strength of the system cannot be evaluated. Many feel that DSS is a good system, but RSA has been available to the public for over 15 years and has been established as the industry's de facto standard.

APPENDIX B

Date	Hosts
Aug.81	213
May.82	235
Aug.83	562
Oct.84	1,024
Oct.85	1,961
Feb.86	2,308
Nov.86	5,089
Dec.87	28,174
Jul.88	33,000
Oct.88	56,000
Jan.89	80,000
Jul.89	130,000
Oct.89	159,000
Oct.90	313,000
Jan.91	376,000
Jul.91	535,000
Oct.91	617,000
Jan.92	727,000
Apr.92	890,000
Jul.92	992,000
Oct.92	1,136,000
Jan.93	1,313,000
Apr.93	1,486,000
Jul.93	1,776,000
Oct.93	2,056,000
Dec.93	2,217,000
Jul.94	3,212,000
Oct.94	3,864,000
Jan.95	4,852,000
Apr.95	5,706,114
Jul.95	6,710,582
Oct.95	7,891,869
Jan.96	9,281,102
Apr.96	10,914,886
Jul.96	12,836,272
Oct.96	15,095,885
Jan.97	17,753,266
Apr.97	20,878,436
Jul.97	24,553,739
Oct.97	28,876,019

Jan.98	33,959,165

(Source: Internet Society, 1996)

Number of Domains

Date	Domains
Jan 93	21,000
Jul 93	26,000
Jan 94	30,000
Jul 94	46,000
Jan 95	71,000
Jul 95	120,000
Jan 96	240,000
Jul 96	488,000

(Source: Network Wizards, 1996)

Growth of the Internet
Networks: 1988-2000
Historical and Projected Values

-----------	Connected Networks ----------		
	USA	non-USA	Total nets
	9	173	
Aug.88	208	9	217
Sep.88	235	9	244
Oct.88	277	14	291
Nov.88	280	33	313
Dec.88	301	33	334
Jan.89	312	34	346
Feb.89	349	35	384
Mar.89	372	38	410
Apr.89	406	61	467
May.89	421	95	516
Jun.89	469	95	564
Jul.89	504	99	603
Aug.89	513	137	650
Sep.89	592	153	745
Oct.89	647	162	809
Nov.89	646	191	837
Dec.89	695	202	897
Jan.90	699	228	927

Feb.90	762	235	997
Mar.90	776	262	1,038
Apr.90	1,224	301	1,525
May.90	1,257	323	1,580
Jun.90	1,301	338	1,639
Jul.90	1,319	408	1,727
Aug.90	1,442	452	1,894
Sep.90	1,503	485	1,988
Oct.90	1,536	527	2,063
Nov.90	1,554	571	2,125
Dec.90	1,575	615	2,190
Jan.91	1,650	688	2,338
Feb.91	1,700	717	2,417
Mar.91	1,744	757	2,501
Apr.91	1,829	793	2,622
May.91	1,881	882	2,763
Jun.91	1,993	989	2,982
Jul.91	2,074	1,012	3,086
Aug.91	2,192	1,066	3,258
Sep.91	2,261	1,128	3,389
Oct.91	2,342	1,214	3,556
Nov.91	2,449	1,302	3,751
Dec.91	2,855	1,450	4,305
Jan.92	3,030	1,496	4,526
Feb.92	3,152	1,588	4,740
Mar.92	3,279	1,697	4,976
Apr.92	3,485	1,806	5,291
May.92	3,604	1,911	5,515
Jun.92	3,737	2,002	5,739
Jul.92	3,898	2,133	6,031
Aug.92	4,112	2,273	6,385
Sep.92	4,304	2,336	6,640
Oct.92	4,788	2,566	7,354
Nov.92	5,022	2,832	7,854
Dec.92	5,366	3,195	8,561
Jan.93	5,699	3,419	9,118
Feb.93	5,904	3,678	9,582
Mar.93	6,394	4,103	10,497
Apr.93	6,790	4,462	11,252
May.93	7,398	4,951	12,349
Jun.93	7,709	5,461	13,170
Jul.93	8,294	5,827	14,121
Aug.93	8,895	6,265	15,160

Sep.93	9,625	7,071	16,696
Oct.93	10,440	7,539	17,979
Nov.93	11,558	8,106	19,664
Dec.93	12,388	9,042	21,430
Jan.94	13,625	9,869	23,494
Feb.94	14,782	10,924	25,706
Mar.94	16,612	11,966	28,578
Apr.94	17,902	12,724	30,626
May.94	18,829	13,541	32,370
Jun.94	19,689	14,362	34,051
Jul.94	20,791	15,362	36,153
Aug.94	21,984	16,323	38,307
Sep.94	22,904	17,073	39,977
Oct.94	23,812	17,708	41,520
Nov.94	24,780	18,103	42,883
Dec.94	25,910	18,779	44,689
Jan.95	26,681	19,637	46,318
-------- Projected -------------			
Feb.95	28,461	21,128	
Mar.95	30,359	22,731	
Apr.95	32,385	24,457	
May.95	34,545	26,313	
Jun.95	36,849	28,310	
Jul.95	39,308	30,459	
Aug.95	41,930	32,771	
Sep.95	44,727	35,259	
Oct.95	47,711	37,935	
Nov.95	50,893	40,814	
Dec.95	54,288	43,912	
Jan.96	57,910	47,245	
Feb.96	61,773	50,832	
Mar.96	65,894	54,690	
Apr.96	70,289	58,841	
May.96	74,978	63,307	
Jun.96	79,980	68,113	
Jul.96	85,315	73,283	
Aug.96	91,007	78,845	
Sep.96	97,077	84,830	
Oct.96	103,553	91,269	

(Source: Internet Society, 1996)

LIST OF REFERENCES

Abadi, M.; P. Gauthier; S. Glassman; M. Manasse; and P. Sobalvarro. The Millicent Protocol for Inexpensive Electronic Commerce. Summer, 1995. (http://www.research.digital.com/src/millicent/papers/millicent-w3 c4/millicent.html)

ActivMedia. "Making Money Online: Independent survey of online business reveals surprising success and rules of the game." September, 1995. (http://www.sun.com/sunworldonline/swol-09-1995/swol-09-webbiz.html)

ActivMedia. "Trends in the World Wide Web Marketplace." February 1, 1996. (http://www.idc.com)

American Information User Survey. "Percent of Internet User Households will to Pay per Month for Electronic Publishing Services." 1994.

Asian Banker. Lafferty Publications Ltd. "Shopping on the Internet.", March 1996.

Astoria Software. "ZipLock Payment System." Astoria Software, 1995. (http://www.ziplock.com)

Back, Adam. "SSL Challenge Broken." (aba@dcs.ex.ac.uk)

Baker, P. "Micro Payment Transfer Protocol (MPTP) Version 0.1." Working Draft, 1996. (http://www.mptp.com)

Bank Administration Institute. "The Information Superhighway and Retail Banking." Bank Administration Institute, 1995.

BankAmerica Corp. "HomeBanking." BankAmerica Corp., 1996. (http://www.bankamerica.com)

Berniker, Mark. "Sony Online Debuts Internet Site." Broadcasting and Cable. Vol. 125, No. 8. February 20, 1995.

Bodley, David N. "South Florida Mall (tm)." 1995. (http://www.inf-tech.com/mall/security/security.htm)

Borenstein, N. "Perils and Pitfalls of Practical CyberCommerce." First Virtual Holdings, Inc. October, 1995. (http://www.fv.com)

Borenstein, N.; M. Rose; E. Stefferud; and L. Stein. The Green Commerce Model: Internet Draft. First Virtual Holdings, Inc. May 29, 1996. (http://www.fv.com)

Bowen, T. "Open Market Lays Foundation for Internet Commerce." December 18, 1995. (http://www.openmarket.com)

Brewer, E.; P. Gauthier; I. Goldberg; D. Wagner. "Basic Flaws in Internet Security and Commerce." (http://http.cs.berkeley.edu/~gauthier/endpoint-security.html)

BroadVision. "Frequently Asked Questions." January, 1996. (http://www.broadvision.com)

BroadVision Press Release. "BroadVision Unleashes the Power of the Internet with Personalized Marketing and Selling." BroadVision, Inc. January 22, 1996. (http://www.broadvision.com)

Busch, Michael D. "Worried About Credit Card Fraud?" Web On-line Magazine for Aviators. 1996. (mbusch@avweb.com)

Business Wire. "BroadVision to Incorporate RSA Encryption Technology into its Interactive Commerce Management System." Business Wire, Inc. September 20, 1995.

Business Wire. "Connect, Inc. Partners with RSA Data Secirity to Set Industry." Business wire, Inc. January 17, 1996.

Business Wire. "Open Market Unleashes Power of the Web with New Class of Software; Major Companies Line Up for Open Market's New Internet Software for Secure Electronic Commerce and Intranet Applications." Business Wire, Inc. March 4, 1996.

Business Wire. "Terisa Systems Announces Availability of SecureWeb Client and Server Toolkit 2.0 for Secure Communications on WWW." Business Wire, Inc. January 16, 1996.

CAFE. "CAFE, The Electronic Wallet for the Information Age." DigiCash Products, 1996. (http://digicash.com/cafe)

Card Trends. "Will SET Kill Card Fraud on the Internet?" American Bankers Association. April, 1996.

Chatterjee, Patrali; Donna L.Hoffman; and Thomas P. Novak. "Commercial Scenarios for the Web: Opportunities and Challenges." Owen School of Management: Vanderbilt University. October 26, 1995. (http://www2000.ogsm.vanderbilt.edu)

Chaum, David. "Achieving Electronic Privacy." DigiCash Publications, 1996. (http://digicash.com/ecash)

Chaum, David testimony for U.S. House of Representatives: Committee on Banking and Financial Services and Subcommittee on Domestic and International Monetary Policy. July 25, 1995.

CheckFree Corp. "The System for Secure Internet Transactions." CheckFree Corp., 1996. (http://www.checkfree.com)

Chen, Pehong. "On-line marketing means getting up close and personal." San Jose Mercury News, Section 8E. February 19, 1996.

Clickshare Access and Payment Service. "Clickshare - How Does It Work?" Clickshare, 1996. (http://www.clickshare.com)

Claymon, Deborah. "Netgravity Teams with Cybercash to Advance Business Opportunities on the Internet." Cybercash Press Release. San Mateo, CA. April 3, 1996. (deborah@nrh.com)

Claymon, Deborah. "Cybercash and Sligos bring Secure Internet Payment to Europe." Press Release. Redwood City, CA. March 18, 1996. (deborah@nrh.com)

CommerceNet Network Services Working Group. Toward Enabling secure Electronic Commerce: The Need for a Revised U.S. Cryptographic Policy. CommerceNet 1996. (http://www.CommerceNet.com)

Connect. "Groundbreaking Market Study Uncovers Real Costs of Online Interactive Commerce." January 15, 1996. (http://www.connectinc.com)

Crede, A. "Electronic Commerce and the Banking Industry: The Requirement and Opportunities for New Payment Systems using the Internet." Science Policy Research Unit, University of Sussex, 1996. (http://www.2000.ogsm.vanderbilt.edu.com)

Computer Security Institute. "Computer Crime Widespread, Many Organizations Unprepared." 1996. (e-mail: prapalus@mfi.com)

Cuneo, Alice Z. "Internet World Show Spurs Online Commerce Debate." Advertising Age. April 17, 1995.

CyberCash Press Release. "Netgravity Teams with CyberCash to Advance Business Opportunities on the Internet." CyberCash, Inc. April 3, 1996. (http://www.cybercash.com/pressreleases)

CyberCash, Inc. "The CyberCash(tm) System: How it Works." June, 1996. (http://www.cybercash.com/cybercash/cyber2.html)

CyberCash, Inc. "The Six Steps in a Secure Internet Credit Card Payment." CyberCash, Inc. CyberCash White Papers, 1996. (http://www.cybercash.com)

Dahl, Kurt. "Commentary: Internet Is Safest Way To Use Your Credit Card." The Seattle Times. September 24, 1995.

Debit Card News. "Debit Users Create An Internet Business Case." Information Access Company, a Thomson Corporation Company Newsletter Database. September 28, 1995.

DigiCash. "DigiCash - Numbers that are Money." DigiCash Publications, 1996. (http://digicash.com/ecash)

EDI News. "Internet Commerce Hung Up On Security: Vendors Rush In Where Merchants, Consumers Fear To Tread." Phillips Business Information, Inc. February 19, 1996.

Eichler, Sara H. and Mary A. Modahl. "The Internet Economy." Forrester Research. Vol. 2, No. 5. September 1, 1995. (http://www.forrester.com/hp_sep95ptr.html)

Electronic Payments International. "The growing impact of the Internet." Lafferty Publications Limited. March, 1996.

Elgamal, Taher. "Commerce on the Internet: Credit Card Payment Applications Over the Internet." Netscape Communications Corporation, Version 1.00, July 14, 1995.

Evans, Judith. "MasterCard-Visa Agreement on Credit Card Security May Make On-Line Commerce Fly." The Washington Post. February 2, 1996.

Europay International. "Europay and IBM Team up for Secure Internet Commerce." Europay International, 1996. (http://www.europay.com)

Fahn, Paul. "Answers to Frequently Asked Questions about Today's Cryptography." RSA Laboratories, 1993. (http://www.rsa.com/rsalabs/faq)

Faulkner & Gray, Inc. "Safety Net." February 26, 1996.

Federal Register. Title 3 - Executive Order 12931 of October 13, 1994. The President Federal Procurement Reform. Vol. 59, No. 199, October 17, 1994.

Find/SVP. "Interactive Consumers." Vol. 2, No. 9. September 1995. (http://etrg.findsvp.com)

Find/SVP. "The American Internet User Survey." 1996. (http://etrg.findsvp.com)

First Union Corp. "First Union and Major Merchants Unveil Smart Card in U.S. Product Launch." First Union Corp., 1996. (http://www.firstunion.com)

First Virtual Holdings Inc. Customer Service Telephone Conversation. August 15, 1996.

First Virtual Holdings Inc. "Information Payment System Summary." First Virtual Holdings, Inc. Information White Paper, 1996. (http://www.firstvirtual.com)

Fletcher, Terry. "Engineering Economy Study: Advertising on the World Wide Web." Universtity of the Pacific, 1996. (http://www.kern.com/~daemonic/econ/econstdy.html)

Flohr, Udo. "Bank Robbers Go Electric." Byte, 1996.

Forrester Research. "Money & Technology Strategies." Volume 1, Number 7. March 1, 1996. (http://www.forrester.com)

Freier, Alan O.; Philip Karlton; Paul C. Kocher. "SSL V3.0." Internet Draft, March 1996. (http://www.netscape.ssl.com)

Fries, V.; J.A. Morell; W. Neal. "Executive Summery of Survey Results." Industrial Technology Institute. May 1995. (www.iti.org/cec/edi-survey/edisurv.html)

Frook, John Evan. "First Internet survey to use random-digit dialing." CMP Publications Inc. 1996.

Gable, Tom. "First Virtual Holdings Indentifies Major Flaw in Software-Based Encryption of Credit Cards." February 7, 1996. (http://www.fv.com)

Garfinkel, Simson L. "Paying through the Net: Virtual credit good at Net sites everywhere." San Jose Mercury News. January 29, 1996. (http://www.firstvirtual.com/pressrel)

Gens, Frank. "What Are the Fortune 500 Doing on the Web?" International Data Corporation. June, 1996. (http://www.idc.research.com/gens4.html)

Gifford, D.; A. Payne; L. Stewart; and G. Treese.·" Payment Switches for Open Networks." Open Market, Inc. 1996. (e-mail: gifford,stewart,payne,treese @openmarket.com)

Global Concepts. "Results of the Survey of Internet Commerce." 1996. (http://www.global concepts.com)

Gray, Matthew. Comprehensive List of Sites. 1995. (http://www.netgen.com/cgi/comprehensive)

Grossman, Mark. "The Bogeyman Won't Get You-The Internet Is Safe Enough For Your Credit Cards." Guru Communications, Inc. 1996.

Gupta, Sunil. "The Fourth WWW Consumer Survey." A Hermes Project, in collaboration with GVU Center's 4th WWW User Survey. 1996.

Hartmann, Peter. "The IDEA Cryptographic Alogorithm, a Successor to DES." European Government Journal. June 1996. (http://www.ascom.ch/Web/systec/press/release2.html)

Hickman, K. "The SSL Protocol, Internet Draft." Netscape Communications Corporation, April, 1995. (http://www.netscape.com/draft/hickman/ssl/00.txt)

Hoffman, Donna L. "Cyberspace to Congress: The Net is Mainstream--and it Votes!" MicroTimes, #148, March 4, 1996.

Hoffman, Donna L. and Thomas P. Novak. "A New Marketing Paradigm for Electronic Commerce." Owen School of Management: Vanderbilt University. February 19, 1996. (http://www.2000.ogsm.vanderbilt.edu)

Hoffman, Donna L.; William D. Kalsbeek; and Thomas P. Novak. "Internet Use in the United States: 1995 Baseline Estimates and Preliminary Market Segments." Owen School of Management: Vanderbilt University. April 12, 1996. (http://www.2000.ogsm.vanderbilt.edu)

Husum, D. "Security Flaw Found in Netscape's Navigator. Fix is in the Works." (http://netscape.com/security.html)

IITA. "Electronic Commerce and the NII." Information Infrastructure Technology and Applications Task Group, National Coordination Office for High Performance Computing and Communications. February, 1994.

InformationWeek. "The Big Picture; The Real Net Security Scandal--Why banks and advertisers need customers to feel the Internet is secure." CMP Publications, Inc. November 27, 1995.

"Infosafe Introduces New Security System for Commercial Transactions on the Internet." February, 1996. (http://www.infosafe.com)

Internet Society. "Interactive Marketing Facts." 1995. (http://www.isa.net/intfacts/market.html)

Internet Society. "Internet Usage and Growth Facts." (ftp://ftp.isoc.org/isoc/charts2/growth).

Intuit, Inc. "Intuit Announces 15 more Financial Institutions to Deliver Online Banking." Quicken Financial Network, 1995. (http://www.intuit.com)

Intuit, Inc. "Intuit to Offer Internet Banking Connection." Quicken Financial Network, 1995. (http://www.intuit.com)

Jaffee, Larry. "Bits & Bytes." DM News. May 20, 1996.

Jaffee, Larry. "Survey: Users Say Tougher 'Net Security Measures Are Needed." DM News. February 5, 1996.

Jones, Russ. "Digital's World-Wide Web Server: A Case Study." Computer Networks & ISDN Systems. Vol. 27, No. 2. November, 1994.

Kaiden, Ethel. "Digital and Cybercash Create Premier Internet Commerce Solution." Press Release. NewYork. March 25, 1996. (kaiden@ljo.dec.com)

Kavanaugh, C. "Smart Card Forum." Davanaugh & Associates, Inc. 1996. (http://www.smartcard.com)

Kent, Stephen. "Privacy-Enhanced Electronic Mail." August, 1996. (http://www.ietf.cnri.reston.va.us/html.charters/pem-charter.html)

Kezar, M. "Logging on to Electronic Media." 1996. (http://electronic.commerce.com)

King, K. "Sequent and Open Market Announce World's Fastest Web Server." March 4, 1996. (http://www.openmarket.com/pressreleases)

Kline, David. "Friction-Free Foolishness." HotWired. September 11, 1995. (http://www.hotwired.com/market/95/37/index1a.html)

Krauskopf, T. "Electronic Commerce Standards for the WWW." Spyglass, Inc. 1994, 1995. (http://www.spyglass.com)

Kristol, David M.; Steven H. Low; Nicholas F. Maxemchuk. "Anonymous Internet Mercantile Protocol." AT&T Bell Laboratories. March 17, 1994. (http://www.ganges.cs.tcd.ie/mepierce/project/bib.html)

Lash, Alex. "Burns Bill Would Ease Encryption Rules." C/Net News. May 2, 1996.

Lieu, S.M. "On Cryptography and Privacy." Netsurfer Focus. Vol. 1, Issue 3. August 21, 1995. (http://www.netsurf.com/nsf/vol/o3/nsf.01.03.html).

"Life on the Line; Credit where Credit is Due." Orange County Register. March 31, 1996.

Linehan, M. and G. Tsudik. "Internet Keyed Payments Protocol (iKP)." IBM Research, July, 1995. (http://www.ibm.com)

Linn, J. "Generic Security Service Application Program Interface, Version 2." August 15, 1996. (http://www.gssv2.com)

Low, Steven H.; Nicholas F. Maxemchuk; Sanjoy Paul. "Anonymous Credit Cards." AT&T Bell Laboratories. November 2, 1994. (http://www.ganges.cs.tcd.ie/mepierce/project/bib.html)

Low, Steven H.; Nicholas F. Maxemchuk; Sanjoy Paul. "Anonymous Credit Cards and its Collusion Analysis." AT&T Bell Laboratories. October 10, 1994. (http://www.ganges.cs.tcd.ie/mepierce/project/bib.html)

Lunt, Penny. "Will SET kill card fraud on the Internet?" American Banking Association ABA Banking Journal. April, 1996.

Lynch, Stephen. "Life On The Line: Credit Where Credit Is Due." Orange County Register. Section K10. March 31, 1996.

M2 Communications. "Steerling Software to provide Internet related electionic commerce services to open market customers." Information Access Company, Thomson Corporation Company. March 5, 1996.

Magid, Lawrence. "Populism Thrives Online." Informationweek. Vol. 514. February 13, 1995.

Matrix News. "Summary of the Results, Second TIC/MIDS Internet Demographic Survey." April 1995. (http://www.mids.org)

Massotto, Tom. "The CommerceNet/Nielson Internet Demographics Survey." October 30, 1995. (http://www.commercenet.com)

Merit Network, Inc. "Internet Growth Statistics." 1995. (ftp://www.nic.merit.edu/nsfnet/statistics)

Merkle, R.C. and M.E. Hellman. "On the security of multiple encryption." Communications of the ACM, Vol. 24. July 1981.

Michalski, Jerry. "Caught in a net of Support." London Sunday Times. June 11, 1995.

Mondex. "Mondex on the Net." 1996. (http://www.mondex.com)

NetBank. "The First National Bank of CyberSpace." 1994. (http://www.netbank.com/netcash)

NetCash. "Public Key Encryption using Pretty Good Privacy (PGP)." 1995. (http://www.netcash.com/pgp)

NetChex Inc. "NetChex - How Does It Work?" 1996. (http://www.netchex.com)

NetChex Inc. "NetChex Security" 1996. (http://www.netchex.com)

NetFare. "NetFare - How Does It Work?" 1995. (http://www.netfare.com)

Netscape Communications Corporation. "Industry Leaders Support Secure Sockets Layer for Internet Security." March 20, 1995. (http://www.netscape.com/pressreleases)

Netscape Communications Corporation. "Key Challenge." September, 1995. (http://www.netscape.com)

Netscape Communications Corporation. "Key Security Overview." Internet Scenarios. 1996. (http://www.netscape.com)

Netscape Communications Corporation. "Netscape Announces Availability of Secure Sockets Layer V3.0 Software Development Toolkit." June 17, 1996. (http://www.netscape.com/pressreleases)

Netscape Communications Corporation. "Potential Vulnerability In Netscape Products." September, 1995. (http://www.netscape.com)

"Netscape flaw puts spotlight on security. Graduate students crack code used to transfer money." The Kansas City Star Co. September 20, 1995.

Network Wizards. "Internet Domain Survey, July 1996." (http://www.nw.com).

New York Times. "How a computer sleuth traced a digital trail." News & Observer Publishing Co. February 15, 1995.

Northwestern Financial Review. "Hip or Hype?" Northwestern Financial Review, February 17, 1996.

O'Conner, Rory J. "FBI Survey Reveals Growth Of Cybercrime." San Jose Mercury News, Section 1E. May 6, 1996.

O'Kelly, R. "Mondex Expected to Gain Worldwide Compatibility with Verifone Systems." Mondex Press Release, May 20, 1996. (http://www.mondex.com/pressreleases)

Open Market. "Premenos and Open Market Announce Strategic OEM Alliance." Concord, CA. March 4, 1996. (http://www.premenos.com/premenos/press/press.html)

Open Market. "The Integrated Commerce Environment." (http://www.openmarket.com/techlib)

Open Market. "The Open Market Commerce Architecture and Its Implementation in Merchant Solution." (http://www.openmarket.com/techlib)

O'Reilly & Associates. "Defining the Internet Opportunity." 1996. (http://gnn.com/gnn/bus/ora/survey)

O'Reilly & Associates. "Internet Commerce Still an Open Field." 1996. (http://gnn.com/gnn/bus/ora/survey)

Pescatore, John "The Future of Cryptography." IDC Government. Interactive Research Service. January 1996.

Power, Kevin. "FBI Survey Finds Many Officials Are Unaware Of System Attacks." Government Computer News, Vol. 15, Number 11. May 27, 1996.

PR Newswire. "Azteq Direct Becomes First Internet Retailer to Issue Debit Cards to ensure Online Security over the Internet." PR Newswire Association, Inc. February 21, 1996.

PR Newswire. "Cyberspace Shopping Predicted to have Impact on Retail Industry." PR Newswire Association, Inc. February 22, 1996.

PR Newswire. "SBT and Checkfree Provide Complete Internet Commerce Solution." PR Newswire Association, Inc. November 22, 1995.

Rescorla, E. and Schiffman, A. "The Secure Hypertext Transfer Protocol: Internet Draft." Enterprise Integration Technologies, December, 1995.

Ricciuti, Mike. "Database Vendors Hawk Wares on Internet." InfoWorld. Vol. 17, No. 2. January 9, 1995.

Rivest, R. "PayWord and MicroMint: Two Simple Micropayment Schemes." MIT Laboratory for Computer Science, May 7, 1996.

Roche, Edward E. "Business Value of Electronic Commerce over Interoperable Networks." Discussion paper for the workshop on interoperability and the economics of Information infrastructure. July, 1995.

Rosenthal, D. "GSS-API for Web Security." Internet Draft, November 1995. (http://www.gssapi.com)

RSA Data Security, Inc. "Public-Key Cryptography Standards (PKCS)." Version 1.5, revised Nov. 1, 1993. (http://www.rsa.com/pub/pkcs/doc).

RSA Laboratories. "RSA Frequently Asked Questions About Today's Cryptography." RSA Data Security, Inc. (http://www.webmaven@rsa.com)

Runge, Bob. "Creating a New Medium for Marketing and Selling." BroadVision, Inc. (http://www.broadvision.com)

Satran, Dick. "In(ternet) crowd is biggest on-line advertiser." San Jose Mercury News. Section E, p.9. December 11, 1995.

Secure Electronic Transaction (SET) Specification. Book 1: Business Description. MasterCard and Visa International. Internet draft, February 23, 1996. (http://www.mastercard.com)

Secure Electronic Transaction (SET) Specification. Book 2: Technical Specifications. MasterCard and Visa International. Internet draft, February 23, 1996. (http://www.mastercard.com)

SecureWare, Inc. Secure Web Platform Whitepaper. SecureWare, Inc. 1995. (http://www.secureware.com/papers)

"Security Alarm." Centaur Communications Ltd. Marketing Week. January 26, 1996.

Security First Network Bank. "Finance on the Web."1996. (http://www.sfnb.com)

Security First Network Bank. "Security White Paper, Information."1996. (http://www.sfnb.com)

Sims, J. "CheckFree and CyberCash Join Forces to Deliver Comprehensive Electronic Commerce Solution." July 13, 1995. (http://www.checkfree.com)

Stein, Lee H. "The Green Commerce Model." May 29, 1995. (http://www.fv.com)

Stone, Keith. "Mitnick Case: 18 Months and Waiting." Los Angeles Daily News. August 13, 1996. (Computer News Daily)

Strohecker, James. "Connect Adds Verisign Digital Certificates to OneServer Internet Software Platform." Connect, Inc. April 29, 1996. (http://www.connect.com/pressreleases)

Strohecker, James. "Connect Announces Solution Partners Program to Speed Delivery of Custom Interactove Commerce Applications." Connect, Inc. March 25, 1996. (http://www.connect.com/pressreleases)

Strohecker, James. "Connect Demonstrates First Implementation of JAVA for Internet-Based Interactive Commerce." Connect, Inc. March 4, 1996. (http://www.connect.com/pressreleases)

Strohecker, James. "Connect Includes CyberCash as Solution Partner, Reinforcing Internet Security of OneServer Platform." Connect, Inc. April 15, 1996. (http://www.connect.com/pressreleases)

Strohecker, James. "Connect Unveils First Internet-Based Order Management Application, Enabling Virtual Sales Channel for Business." Connect, Inc. May 14, 1996. (http://www.connect.com/pressreleases)

Strohecker, James. "Leading Provider of Transaction Card Processing Selects Connect OneServer OrderStream Software as a Solution for Advanced Internet Merchant Services." Connect, Inc. May 21, 1996. (http://www.connect.com/pressreleases)

Strohecker, James. "Logica Joins Connect as Solution Partner to Implement OneServer as the Standard Platform for Multimedia Interactive Commerce." Connect, Inc. April 8, 1996.
(http://www.connect.com/pressreleases)

"Superhighway robbers hit banks." The News and Observer Publishing Co. September 3, 1995.

The American Banker. "On the Question of Internet Security, A Three-Sided Debate." April 15, 1996.

Tischler, Richard. "Europay and IBM Team Up For Secure Internet Commerce." Waterloo Press Release. June 14, 1995.

Tsudik, G. "Zurich iKP Prototype (ZIP)." IBM Research. January 29, 1996.

Unruh, Bill. "Cryptography." July 20, 1996.
(http://axion.physics.ubc.ca/crypt.html#DH).

Verisign, Inc. "Introduction to Cryptography." February 9, 1996.
(http://www.verisign.com/techdoc).

Visa. "Visa Establishes International Consortium for Electronic Purse Specifications." 1996. (http://www.visa.com)

Wallace, David J. "Shopping Online: A Sticky Business." Advertising Age. April 10, 1995.

Wayner, Peter. Digital Cash: Commerce on the Net. Academic Press, Inc. 1996.

WebTrack. "Top Web Advertisers." 1996. (http://www.webtrack.com/research.html)

Wells Fargo. "Encrypted Online Banking Sessions." Wells Fargo, 1996. (http://www.wellsfargo.com)

Wilson, Richenda. "Security Alarm." Centaur Communications Ltd. Marketing Week. January 26, 1996.

Wiggins, Richard W. "Growth of the Internet: An Overview of a Complicated Subject." September 5, 1995. (http://www.isa.com)

Wilder, Clinton. "Online Transactions: Pouring Cash into the Internet." Information Week. January 1, 1996. (http://techweb.cmp.com/iwk).

Ylonen, Tatu. "Cryptographic Algorithms." 1996. (e-mail: ylo@cs.hut.fi).

Ziegler, Bart. "Shares of Homes with PCs Rises to 31% in Poll." Wall Street Journal. Section B, Col. 1, p.5. February 6, 1995.

INITIAL DISTRIBUTION LIST

No. of copies

1. Defense Technical Information Center...2
8725 John J. Kingman Rd., STE 0944
Ft. Belvoir, VA 22060-6218

2. Dudley Knox Library 2
Naval Postgraduate School
411 Dyer Rd.
Monterey, CA 93943-5101

3. David K. Flick, Lt USN 1
615 E. Grant Ave.
Altoona, PA 16602

4. Barry A. Frew 1
Associate Professor Code SM/fw
Naval Postgraduate School
Monterey, CA 93940-5000

5. Charles R. Gillum, Lt USN 2
8706 Crystal Rock Lane
Laurel, MD 20708

6. William J. Haga 1
Professor Code SM/hg
Naval Postgraduate School
Monterey, CA 93940-5000